Histórico de vulnerabilidades de Setembro do 2016

Semana 26/09/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aternity -- aternity	The web server in Aternity 9 and earlier does not require authentication for getMBeansFromURL loading of Java MBeans, which allows remote attackers to execute arbitrary Java code by registering MBeans.	29/09/2016	9.3	CVE-2016-5062
hp -- network_automation	HP Network Automation Software 9.1x, 9.2x, 10.0x before 10.00.02.01, and 10.1x before 10.11.00.01 allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	29/09/2016	7.5	CVE-2016-4385
isc -- bind	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.	28/09/2016	7.8	CVE-2016-2776
libgd -- libgd	Integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calls.	28/09/2016	7.5	CVE-2016-7568
redhat -- jboss_operations_network	The server in Red Hat JBoss Operations Network (JON), when SSL authentication is not configured for JON server / agent communication, allows remote attackers to execute arbitrary code via a crafted HTTP request, related to message deserialization. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-3737.	27/09/2016	9.0	CVE-2016-6330
sap -- trex	An unspecified function in SAP TREX 7.10 Revision 63 allows remote attackers to execute arbitrary OS commands via unknown vectors, aka SAP Security Note 2203591.	27/09/2016	10.0	CVE-2016-6137
adobe -- digital_editions	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4263.	26/09/2016	10.0	CVE-2016-6980
citrix -- linux_virtual_delivery_agent	Citrix Linux Virtual Delivery Agent (aka VDA, formerly Linux Virtual Desktop) before 1.4.0 allows local users to gain root privileges via unspecified vectors.	26/09/2016	7.2	CVE-2016-6276
huawei -- anyoffice_secureapp	Huawei AnyMail before 2.6.0301.0060 allows remote attackers to cause a denial of service (application crash) via a crafted compressed email attachment.	26/09/2016	7.1	CVE-2016-6826
huawei -- honor6_firmware	The video driver in Huawei Mate S smartphones with software CRR-TL00 before CRR-TL00C01B362, CRR-UL20 before CRR-UL20C00B362, CRR-CL00 before CRR-CL00C92B362, and CRR-CL20 before CRR-CL20C92B362; P8 smartphones with software GRA-TL00 before GRA-TL00C01B366, GRA-UL00 before GRA-UL00C00B366, GRA-UL10 before GRA-UL10C00B366, and GRA-CL00 before GRA-CL00C92B366; and Honor 6 and Honor 6 Plus smartphones with software before 6.9.16 allows attackers to cause a denial of service (device reboot) via a crafted application.	26/09/2016	7.1	CVE-2016-8279
iperf_project -- iperf	The parse_string function in cjson.c in the cJSON library mishandles UTF8/16 strings, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a non-hex character in a JSON string, which triggers a heap-based buffer overflow.	26/09/2016	7.5	CVE-2016-4303
openssl -- openssl	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.	26/09/2016	7.8	CVE-2016-6304
openssl -- openssl	statem/statem_dtls.c in the DTLS implementation in OpenSSL 1.1.0 before 1.1.0a allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted DTLS messages.	26/09/2016	7.1	CVE-2016-6308
openssl -- openssl	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote attackers to cause a denial of service (use-after-free) or possibly execute arbitrary code via a crafted TLS session.	26/09/2016	10.0	CVE-2016-6309
openstack -- mitaka-murano	OpenStack Murano before 1.0.3 (liberty) and 2.x before 2.0.1 (mitaka), Murano-dashboard before 1.0.3 (liberty) and 2.x before 2.0.1 (mitaka), and python-muranoclient before 0.7.3 (liberty) and 0.8.x before 0.8.5 (mitaka) improperly use loaders inherited from yaml.Loader when parsing MuranoPL and UI files, which allows remote attackers to create arbitrary Python objects and execute arbitrary code via crafted extended YAML tags in UI definitions in packages.	26/09/2016	7.5	CVE-2016-4972
powerdns -- authoritative_server	PowerDNS (aka pdns) Authoritative Server before 4.0.1 allows remote primary DNS servers to cause a denial of service (memory exhaustion and secondary DNS server crash) via a large (1) AXFR or (2) IXFR response.	26/09/2016	7.1	CVE-2016-6172
apple -- apple_tv	libxml2 in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.	25/09/2016	10.0	CVE-2016-4658
apple -- mac_os_x	The Apache HTTP Server in Apple OS X before 10.12 and OS X Server before 5.2 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted CGI client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue, a related issue to CVE-2016-5387.	25/09/2016	7.5	CVE-2016-4694
apple -- mac_os_x	AppleEFIRuntime in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app.	25/09/2016	9.3	CVE-2016-4696
apple -- mac_os_x	Apple HSSPI Support in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4697
apple -- iphone_os	AppleMobileFileIntegrity in Apple iOS before 10 and OS X before 10.12 mishandles process entitlement and Team ID values in the task port inheritance policy, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	25/09/2016	9.3	CVE-2016-4698
apple -- mac_os_x	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4700.	25/09/2016	9.3	CVE-2016-4699
apple -- mac_os_x	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4699.	25/09/2016	9.3	CVE-2016-4700
apple -- apple_tv	Audio in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	25/09/2016	10.0	CVE-2016-4702
apple -- mac_os_x	Bluetooth in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4703
apple -- mac_os_x	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4710.	25/09/2016	7.2	CVE-2016-4709
apple -- mac_os_x	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4709.	25/09/2016	7.2	CVE-2016-4710
apple -- apple_tv	CoreCrypto in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted app.	25/09/2016	9.3	CVE-2016-4712
apple -- mac_os_x	diskutil in DiskArbitration in Apple OS X before 10.12 allows local users to gain privileges via unspecified vectors.	25/09/2016	7.2	CVE-2016-4716
apple -- mac_os_x	Intel Graphics Driver in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4723
apple -- iphone_os	IOAcceleratorFamily in Apple iOS before 10 and OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app.	25/09/2016	9.3	CVE-2016-4724
apple -- apple_tv	IOAcceleratorFamily in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4726
apple -- mac_os_x	IOThunderboltFamily in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4727
apple -- safari	WebKit in Apple iOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4731.	25/09/2016	9.3	CVE-2016-4729
apple -- safari	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4733, CVE-2016-4734, and CVE-2016-4735.	25/09/2016	9.3	CVE-2016-4730
apple -- safari	WebKit in Apple iOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4729.	25/09/2016	9.3	CVE-2016-4731
apple -- safari	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4734, and CVE-2016-4735.	25/09/2016	9.3	CVE-2016-4733
apple -- safari	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4735.	25/09/2016	9.3	CVE-2016-4734
apple -- safari	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4734.	25/09/2016	9.3	CVE-2016-4735
apple -- mac_os_x	libarchive in Apple OS X before 10.12 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted file.	25/09/2016	9.3	CVE-2016-4736
apple -- safari	WebKit in Apple iOS before 10, Safari before 10, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	25/09/2016	9.3	CVE-2016-4737
apple -- apple_tv	libxslt in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	25/09/2016	9.3	CVE-2016-4738
apple -- iphone_os	S2 Camera in Apple iOS before 10 and OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4750
apple -- apple_tv	Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 mishandle signed disk images, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	25/09/2016	9.3	CVE-2016-4753
apple -- apple_tv	The kernel in Apple OS X before 10.12, tvOS before 10, and watchOS before 3 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	25/09/2016	7.2	CVE-2016-4775
apple -- apple_tv	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (invalid pointer dereference) via a crafted app.	25/09/2016	9.3	CVE-2016-4777
apple -- apple_tv	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/09/2016	9.3	CVE-2016-4778
dexis -- imaging_suite	DEXIS Imaging Suite 10 has a hardcoded password for the sa account, which allows remote attackers to obtain administrative access by entering this password in a DEXIS_DATA SQL Server session.	24/09/2016	10.0	CVE-2016-6532
moxa -- active_opc_server	Unquoted Windows search path vulnerability in Moxa Active OPC Server before 2.4.19 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory.	24/09/2016	7.2	CVE-2016-5793
opendental -- opendental	** DISPUTED ** Open Dental 16.1 and earlier has a hardcoded MySQL root password, which allows remote attackers to obtain administrative access by leveraging access to intranet TCP port 3306. NOTE: the vendor disputes this issue, stating that the "vulnerability note ... is factually false ... there is indeed a default blank password, but it can be changed ... We recommend that users change it, each customer receives direction."	24/09/2016	7.5	CVE-2016-6531

Semana 19/09/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artifex -- mupdf	Heap-based buffer overflow in the pdf_load_mesh_params function in pdf/pdf-shade.c in MuPDF allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a large decode array.	22/09/2016	7.5	CVE-2016-6525
cisco -- cloud_services_platform_2100	The web-based GUI in Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote authenticated administrators to execute arbitrary OS commands as root via crafted platform commands, aka Bug ID CSCva00541.	22/09/2016	9.0	CVE-2016-6373
cisco -- cloud_services_platform_2100	Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote attackers to execute arbitrary code via a crafted dnslookup command in an HTTP request, aka Bug ID CSCuz89093.	22/09/2016	7.5	CVE-2016-6374
cisco -- email_security_appliance	Cisco IronPort AsyncOS 9.1.2-023, 9.1.2-028, 9.1.2-036, 9.7.2-046, 9.7.2-047, 9.7.2-054, 10.0.0-124, and 10.0.0-125 on Email Security Appliance (ESA) devices, when Enrollment Client before 1.0.2-065 is installed, allows remote attackers to obtain root access via a connection to the testing/debugging interface, aka Bug ID CSCvb26017.	22/09/2016	10.0	CVE-2016-6406
cisco -- ios	iox in Cisco IOS, possibly 15.6 and earlier, and IOS XE, possibly 3.18 and earlier, allows local users to execute arbitrary IOx Linux commands on the guest OS via crafted iox command-line options, aka Bug ID CSCux59223.	22/09/2016	7.2	CVE-2016-6414
huawei -- usg2100_firmware	Buffer overflow in the Authentication, Authorization and Accounting (AAA) module in Huawei USG2100, USG2200, USG5100, and USG5500 unified security gateways with software before V300R001C10SPC600 allows remote authenticated RADIUS servers to execute arbitrary code by sending a crafted EAP packet.	22/09/2016	7.1	CVE-2016-6669
lenovo -- bios	The BIOS for Lenovo ThinkCentre E93, M6500t/s, M6600, M6600q, M6600t/s, M73p, M800, M83, M8500t/s, M8600t/s, M900, M93, and M93P devices; ThinkServer RQ940, RS140, TS140, TS240, TS440, and TS540 devices; and ThinkStation E32, P300, and P310 devices might allow local users or physically proximate attackers to bypass the Secure Boot protection mechanism by leveraging an AMI test key.	22/09/2016	7.2	CVE-2016-5247
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	22/09/2016	7.5	CVE-2016-5256
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	22/09/2016	7.5	CVE-2016-5257

Histórico de vulnerabilidades de Setembro do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	Heap-based buffer overflow in the nsCaseTransformTextRunFactory::TransformString function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to cause a denial of service (boolean out-of-bounds write) or possibly have unspecified other impact via Unicode characters that are mishandled during text conversion.	22/09/2016	7.5	CVE-2016-5270
mozilla -- firefox	Use-after-free vulnerability in the nsFrameManager::CaptureFrameState function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between restyling and the Web Animations model implementation.	22/09/2016	7.5	CVE-2016-5274
mozilla -- firefox	Use-after-free vulnerability in the mozilla::a11y::DocAccessible::ProcessInvalidationList function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an aria-owns attribute.	22/09/2016	7.5	CVE-2016-5276
mozilla -- firefox	Use-after-free vulnerability in the nsRefreshDriver::Tick function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging improper interaction between timeline destruction and the Web Animations model implementation.	22/09/2016	7.5	CVE-2016-5277
mozilla -- firefox	Use-after-free vulnerability in the mozilla::nsTextNodeDirectionalityMap::RemoveElementFromMap function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code via bidirectional text.	22/09/2016	7.5	CVE-2016-5280
mozilla -- firefox	Use-after-free vulnerability in the DOMSVGLength class in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between JavaScript code and an SVG document.	22/09/2016	7.5	CVE-2016-5281
redhat -- quickstart_cloud_installer	Red Hat QuickStart Cloud Installer (QCI) uses world-readable permissions for /etc/qci/answers, which allows local users to obtain the root password for the deployed system by reading the file.	22/09/2016	7.2	CVE-2016-6322
apache -- cxf_fediz	The application plugins in Apache CXF Fediz 1.2.x before 1.2.3 and 1.3.x before 1.3.1 do not match SAML AudienceRestriction values against configured audience URIs, which might allow remote attackers to have bypass intended restrictions and have unspecified other impact via a crafted SAML token with a trusted signature.	21/09/2016	7.5	CVE-2016-4464
flex_project -- flex	Heap-based buffer overflow in the yy_get_next_buffer function in Flex before 2.6.1 might allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via vectors involving num_to_read.	21/09/2016	7.5	CVE-2016-6354
fortinet -- fortiwan	Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users with access to the nslookup functionality to execute arbitrary commands with root privileges via the graph parameter to diagnosis_control.php.	21/09/2016	9.0	CVE-2016-4965
huawei -- ws331a_router_firmware	Multiple cross-site request forgery (CSRF) vulnerabilities in Huawei WS331a routers with software before WS331a-10 V100R001C01B112 allow remote attackers to hijack the authentication of administrators for requests that (1) restore factory settings or (2) reboot the device via unspecified vectors.	21/09/2016	7.1	CVE-2016-6158
libarchive -- libarchive	Integer overflow in the ISO9660 writer in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a buffer overflow.	21/09/2016	7.5	CVE-2016-6250
openjpeg -- openjpeg	Use-after-free vulnerability in the opj_j2k_write_mco function in j2k.c in OpenJPEG before 2.1.1 allows remote attackers to have unspecified impact via unknown vectors.	21/09/2016	7.5	CVE-2015-8871
xen -- xen	Xen 4.5.3, 4.6.3, and 4.7.x allow local HVM guest OS administrators to overwrite hypervisor memory and consequently gain host OS privileges by leveraging mishandling of instruction pointer truncation during emulation.	21/09/2016	7.2	CVE-2016-7093
xen -- xen	Use-after-free vulnerability in the FIFO event channel code in Xen 4.4.x allows local guest OS administrators to cause a denial of service (host crash) and possibly execute arbitrary code or obtain sensitive information via an invalid guest frame number.	21/09/2016	7.2	CVE-2016-7154
dentsply_sirona -- cdr_dicom	Dentsply Sirona (formerly Schick) CDR Dicom S and earlier has default passwords for the sa and cdr accounts, which allows remote attackers to obtain administrative access by leveraging knowledge of these passwords.	20/09/2016	10.0	CVE-2016-6530
emc -- avamar_server	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain root privileges by leveraging admin access and entering a sudo command.	20/09/2016	7.2	CVE-2016-0905
emc -- vnx1_oe_firmware	The SMB service in EMC VNXe, VNX1 File OE before 7.1.80.3, and VNX2 File OE before 8.1.9.155 does not prevent duplicate NTLM challenge-response nonces, which makes it easier for remote attackers to execute arbitrary code, or read or write to files, via a series of authentication requests, a related issue to CVE-2010-0231.	20/09/2016	7.5	CVE-2016-0917
emc -- avamar_server	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain root access via a crafted parameter to a command that is available in the sudo configuration.	20/09/2016	7.2	CVE-2016-0920
hp -- loadrunner	HPE Performance Center before 12.50 and LoadRunner before 12.50 allow remote attackers to cause a denial of service via unspecified vectors.	20/09/2016	9.0	CVE-2016-4384
mariadb -- mariadb	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib.	20/09/2016	10.0	CVE-2016-6662
apple -- xcode	otool in Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4705.	18/09/2016	7.2	CVE-2016-4704
apple -- xcode	otool in Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4704.	18/09/2016	7.2	CVE-2016-4705
aver -- eh6108h+_firmware	AVer Information EH6108H+ devices with firmware X9.03.24.00.07l have hardcoded accounts, which allows remote attackers to obtain root access by leveraging knowledge of the credentials and establishing a TELNET session.	18/09/2016	10.0	CVE-2016-6535
aver -- eh6108h+_firmware	The /setup URI on AVer Information EH6108H+ devices with firmware X9.03.24.00.07l allows remote attackers to bypass intended page-access restrictions or modify passwords by leveraging knowledge of a handle parameter value.	18/09/2016	10.0	CVE-2016-6536
cisco -- webex_meetings_server	Cisco WebEx Meetings Server 2.6 allows remote attackers to cause a denial of service (CPU consumption) by repeatedly accessing the account-validation component of an unspecified service, aka Bug ID CSCuy92704.	18/09/2016	7.8	CVE-2016-1483
cisco -- unified_computing_system	UCS Manager and UCS 6200 Fabric Interconnects in Cisco Unified Computing System (UCS) through 3.0(2d) allow local users to obtain OS root access via crafted CLI input, aka Bug ID CSCuz91263.	18/09/2016	7.2	CVE-2016-6402
rockwellautomation -- rslogix_500_professional_edition	Buffer overflow in Rockwell Automation RSLogix Micro Starter Lite, RSLogix Micro Developer, RSLogix 500 Starter Edition, RSLogix 500 Standard Edition, and RSLogix 500 Professional Edition allows remote attackers to execute arbitrary code via a crafted RSS project file.	18/09/2016	9.3	CVE-2016-5814
yokogawa -- stardom_fcn/fcj	Yokogawa STARDOM FCN/FCJ controller R1.01 through R4.01 does not require authentication for Logic Designer connections, which allows remote attackers to reconfigure the device or cause a denial of service via a (1) stop application program, (2) change value, or (3) modify application command.	18/09/2016	7.5	CVE-2016-4860
cisco -- webex_meetings_server	Cisco WebEx Meetings Server 2.6 allows remote attackers to execute arbitrary commands by injecting these commands into an application script, aka Bug ID CSCuy83130.	17/09/2016	9.3	CVE-2016-1482
icu_project -- international_components_for_unicode	Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a lone locale string.	17/09/2016	7.5	CVE-2016-7415
php -- php	ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.	17/09/2016	7.5	CVE-2016-7411
php -- php	Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.	17/09/2016	7.5	CVE-2016-7413
php -- php	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.	17/09/2016	7.5	CVE-2016-7414
php -- php	ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.	17/09/2016	7.5	CVE-2016-7417
pivotal -- cloud_foundry_elastic_runtime	Pivotal Cloud Foundry (PCF) Elastic Runtime before 1.6.34 and 1.7.x before 1.7.12 places 169.254.0.0/16 in the all_open Application Security Group, which might allow remote attackers to bypass intended network-connectivity restrictions by leveraging access to the 169.254.169.254 address.	17/09/2016	7.5	CVE-2016-0896
pivotal -- operations_manager	Pivotal Cloud Foundry (PCF) Ops Manager before 1.6.17 and 1.7.x before 1.7.8, when vCloud or vSphere is used, does not properly enable SSH access for operators, which has unspecified impact and remote attack vectors.	17/09/2016	7.5	CVE-2016-0897
pivotal -- rabbitmq	The metrics-collection component in RabbitMQ for Pivotal Cloud Foundry (PCF) 1.6.x before 1.6.4 logs command lines of failed commands, which might allow context-dependent attackers to obtain sensitive information by reading the log data, as demonstrated by a syslog message that contains credentials from a command line.	17/09/2016	7.8	CVE-2016-0929
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.	16/09/2016	10.0	CVE-2016-6937
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4255.	16/09/2016	10.0	CVE-2016-6938
otrs -- faq	Multiple SQL injection vulnerabilities in the FAQ package 2.x before 2.3.6, 4.x before 4.0.5, and 5.x before 5.0.5 in Open Ticket Request System (OTRS) allow remote attackers to execute arbitrary SQL commands via crafted search parameters.	16/09/2016	9.0	CVE-2016-5843

Semana 12/09/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4256
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4257
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4258
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4259
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4261, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4260
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, and CVE-2016-4262.	16/09/2016	10.0	CVE-2016-4261
adobe -- digital_editions	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, and CVE-2016-4261.	16/09/2016	10.0	CVE-2016-4262
adobe -- digital_editions	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors.	16/09/2016	10.0	CVE-2016-4263
openssl -- openssl	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.	16/09/2016	7.5	CVE-2016-2182
openssl -- openssl	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.	16/09/2016	7.5	CVE-2016-6303
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-4272
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284. CVE-2016-4285. CVE-2016-6922. and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4274

Histórico de vulnerabilidades de Setembro do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4275
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4276
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-4279
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4280
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4281
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4282
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4283
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4284
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-4285
adobe -- flash_player	Integer overflow in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors.	14/09/2016	10.0	CVE-2016-4287
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6921
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-6922
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931. and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6923
adobe -- flash_player	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6924.	14/09/2016	10.0	CVE-2016-6924
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930. CVE-2016-6931. and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6925
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6926
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6929, CVE-2016-6930. CVE-2016-6931. and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6927
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6929
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6931, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6930
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6932.	14/09/2016	10.0	CVE-2016-6931
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6931.	14/09/2016	10.0	CVE-2016-6932
microsoft -- edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3330.	14/09/2016	7.6	CVE-2016-3294
microsoft -- edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3294.	14/09/2016	7.6	CVE-2016-3330
microsoft -- windows_10	The SMBv1 server 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 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Authenticated Remote Code Execution Vulnerability."	14/09/2016	9.0	CVE-2016-3345
microsoft -- windows_10	Microsoft Windows 10 Gold, 1511, and 1607 does not properly enforce permissions, which allows local users to obtain Administrator access via a crafted DLL, aka "Windows Permissions Enforcement Elevation of Privilege Vulnerability."	14/09/2016	7.2	CVE-2016-3346
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."	14/09/2016	9.3	CVE-2016-3348
microsoft -- windows_10	The kernel-mode drivers in Microsoft 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."	14/09/2016	7.2	CVE-2016-3349
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-2016-3377.	14/09/2016	7.6	CVE-2016-3350
microsoft -- windows_10	The Graphics Device Interface (GDI) 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 allows local users to gain privileges via a crafted application, aka "GDI Elevation of Privilege Vulnerability."	14/09/2016	7.2	CVE-2016-3355
microsoft -- windows_10	The Graphics Device Interface (GDI) in Microsoft Windows 10 1607 allows remote attackers to execute arbitrary code via a crafted document. aka "GDI Remote Code Execution Vulnerability."	14/09/2016	9.3	CVE-2016-3356
microsoft -- office	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office 2016, Word for Mac 2011, Word 2016 for Mac, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, SharePoint Server 2013 SP1, Excel Automation Services on SharePoint Server 2013 SP1, Word Automation Services on SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3357
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3358
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3359
microsoft -- office_compatibility_pack	Microsoft PowerPoint 2007 SP3, PowerPoint 2010 SP2, PowerPoint 2013 SP1, PowerPoint 2013 RT SP1, PowerPoint 2016 for Mac, Office Compatibility Pack SP3, PowerPoint Viewer, SharePoint Server 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3360
microsoft -- excel	Microsoft Excel 2010 SP2 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3361
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3365.	14/09/2016	9.3	CVE-2016-3362
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3381.	14/09/2016	9.3	CVE-2016-3363
microsoft -- visio	Microsoft Visio 2016 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3364
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Automation Services on SharePoint Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3362.	14/09/2016	9.3	CVE-2016-3365
microsoft -- silverlight	StringBuilder in Microsoft Silverlight 5 before 5.1.50709.0 does not properly allocate memory for string-insert and string-append operations, which allows remote attackers to execute arbitrary code via a crafted web site, aka "Microsoft Silverlight Memory Corruption Vulnerability."	14/09/2016	9.3	CVE-2016-3367
microsoft -- windows_10	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 remote authenticated users to execute arbitrary code by leveraging a domain account to make a crafted request, aka "Windows Remote Code Execution Vulnerability."	14/09/2016	9.0	CVE-2016-3368
microsoft -- windows_10	Microsoft Windows 10 Gold and 1511 allows attackers to cause a denial of service via unspecified vectors, aka "Windows Denial of Service Vulnerability."	14/09/2016	7.8	CVE-2016-3369
microsoft -- internet_explorer	The OLE Automation mechanism and VBScript scripting engine in Microsoft Internet Explorer 9 through 11, 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 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."	14/09/2016	7.6	CVE-2016-3375
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-2016-3350.	14/09/2016	7.6	CVE-2016-3377

Histórico de vulnerabilidades de Setembro do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3363.	14/09/2016	9.3	CVE-2016-3381
cisco -- ace_application_control_engine_module_a1	Cisco ACE30 Application Control Engine Module through A5 3.3 allow remote attackers to cause a denial of service (device reload) via crafted (1) SSL or (2) TLS packets, aka Bug ID CSCvb16317.	12/09/2016	7.8	CVE-2016-6399
cisco -- spa300_series_ip_phone_firmware	The HTTP framework on Cisco SPA300, SPA500, and SPA51x devices allows remote attackers to cause a denial of service (device outage) via a series of malformed HTTP requests, aka Bug ID CSCut67385.	11/09/2016	7.8	CVE-2016-1469
google -- android	Buffer overflow in drivers/soc/qcom/subsystem_restart.c in the Qualcomm subsystem driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application that provides a long string, aka Android internal bug 28675151 and Qualcomm internal bug CR1022641.	11/09/2016	9.3	CVE-2016-3858
google -- android	The Qualcomm camera driver in Android before 2016-09-05 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28815326 and Qualcomm internal bug CR1024641.	11/09/2016	9.3	CVE-2016-3859
google -- android	LibUtils in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 mishandles conversions between Unicode character encodings with different encoding widths, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow) via a crafted file, aka internal bug 29250543.	11/09/2016	9.3	CVE-2016-3861
google -- android	media/ExifInterface.java 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 2016-09-01 does not properly interact with the use of static variables in libjhead_jni, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 29270469.	11/09/2016	9.3	CVE-2016-3862
google -- android	The Qualcomm radio interface layer in Android before 2016-09-05 on Nexus 5, Nexus 5X, Nexus 6, Nexus 6P, and Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28823714 and Qualcomm internal bug CR913117.	11/09/2016	9.3	CVE-2016-3864
google -- android	The Synaptics touchscreen driver in Android before 2016-09-05 on Nexus 5X and 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28799389.	11/09/2016	9.3	CVE-2016-3865
google -- android	The Qualcomm sound driver in Android before 2016-09-05 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28868303 and Qualcomm internal bug CR1032820.	11/09/2016	9.3	CVE-2016-3866
google -- android	The Qualcomm IPA driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28919863 and Qualcomm internal bug CR1037897.	11/09/2016	9.3	CVE-2016-3867
google -- android	The Qualcomm power driver in Android before 2016-09-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28967028 and Qualcomm internal bug CR1032875.	11/09/2016	9.3	CVE-2016-3868
google -- android	The Broadcom Wi-Fi driver in Android before 2016-09-05 on Nexus 5, Nexus 6, Nexus 6P, Nexus 9, Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29009982 and Broadcom internal bug RBP96070.	11/09/2016	9.3	CVE-2016-3869
google -- android	omx/SimpleSoftOMXComponent.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 does not prevent input-port changes, which allows attackers to gain privileges via a crafted application, aka internal bug 29421804.	11/09/2016	9.3	CVE-2016-3870
google -- android	Multiple buffer overflows in codecs/mp3dec/SoftMP3.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allow attackers to gain privileges via a crafted application, aka internal bug 29422022.	11/09/2016	9.3	CVE-2016-3871
google -- android	Buffer overflow in codecs/on2/dec/SoftVPX.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows attackers to gain privileges via a crafted application, aka internal bug 29421675.	11/09/2016	9.3	CVE-2016-3872
google -- android	The NVIDIA kernel in Android before 2016-09-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 29518457.	11/09/2016	9.3	CVE-2016-3873
google -- android	CORE/HDD/src/wlan_hdd_wext.c in the Qualcomm Wi-Fi driver in Android before 2016-09-05 on Nexus 5X devices does not properly validate the arguments array, which allows attackers to gain privileges via a crafted application that sends a WE_UNIT_TEST_CMD command, aka Android internal bug 29944562 and Qualcomm internal bug CR997797.	11/09/2016	9.3	CVE-2016-3874
google -- android	server/wm/WindowManagerService.java in Android 6.x before 2016-09-01 does not enforce the DISALLOW_SAFE_BOOT setting, which allows physically proximate attackers to bypass intended access restrictions and boot to safe mode via unspecified vectors, aka internal bug 26251884.	11/09/2016	7.2	CVE-2016-3875
google -- android	providers/settings/SettingsProvider.java in Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the SAFE_BOOT_DISALLOWED protection mechanism and boot to safe mode via the Android Debug Bridge (adb) tool, aka internal bug 29900345.	11/09/2016	7.2	CVE-2016-3876
google -- android	Unspecified vulnerability in Android before 2016-09-01 has unknown impact and attack vectors.	11/09/2016	10.0	CVE-2016-3877
google -- android	decoder/ih264d_api.c in mediaserver in Android 6.x before 2016-09-01 mishandles the case of decoding zero MBs, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 29493002.	11/09/2016	7.1	CVE-2016-3878
google -- android	arm-wt-22k/lib_src/eas_mdls.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 2016-09-01 allows remote attackers to cause a denial of service (NULL pointer dereference, and device hang or reboot) via a crafted media file, aka internal bug 29770686.	11/09/2016	7.1	CVE-2016-3879
google -- android	Multiple buffer overflows in rtsp/ASessionDescription.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allow remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 25747670.	11/09/2016	7.1	CVE-2016-3880
google -- android	The decoder_peek_si_internal function in vp8/vp9_dx_iface.c in libvpx in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows remote attackers to cause a denial of service (buffer over-read, and device hang or reboot) via a crafted media file, aka internal bug 30013856.	11/09/2016	7.1	CVE-2016-3881
google -- android	debuggerd/debuggerd.cpp in Debuggerd in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 mishandles the interaction between PTRACE_ATTACH operations and thread exits, which allows attackers to gain privileges via a crafted application, aka internal bug 29555636.	11/09/2016	9.3	CVE-2016-3885
google -- android	systemui/statusbar/phone/QuickStatusBarHeader.java in the System UI Tuner in Android 7.0 before 2016-09-01 does not prevent tuner changes on the lockscreen, which allows physically proximate attackers to gain privileges by modifying a setting, aka internal bug 30107438.	11/09/2016	7.2	CVE-2016-3886
google -- android	Android 6.x before 2016-09-01 and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism by accessing (1) an external tile from a system application, (2) the help feature, or (3) the Settings application during a pre-setup stage, aka internal bug 29194585.	11/09/2016	7.2	CVE-2016-3889
google -- android	The Java Debug Wire Protocol (JDWP) implementation in adb/sockets.cpp 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 2016-09-01 mishandles socket close operations, which allows attackers to gain privileges via a crafted application, aka internal bug 28347842.	11/09/2016	7.6	CVE-2016-3890
google -- android	OMXCodec.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, 6.x before 2016-09-01, and 7.0 before 2016-09-01 does not validate a certain pointer, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 29421811.	11/09/2016	7.1	CVE-2016-3899
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	11/09/2016	7.5	CVE-2016-5167
php -- php	ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.	11/09/2016	7.5	CVE-2016-7124
php -- php	The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.	11/09/2016	7.5	CVE-2016-7126
php -- php	The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.	11/09/2016	7.5	CVE-2016-7127
php -- php	The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.	11/09/2016	7.5	CVE-2016-7129
php -- php	ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is mishandled in a curl_escape call.	11/09/2016	7.5	CVE-2016-7134

Semana 05/09/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortiswitch	Fortinet FortiSwitch FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW-424D, FSW-424D-POE, FSW-424D-FPOE, FSW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW-524D, FSW-524D-FPOE, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D, and FSW-R-112D-POE models, when in FortiLink managed mode and upgraded to 3.4.1, might allow remote attackers to bypass authentication and gain administrative access via an empty password for the rest_admin account.	09/09/2016	10.0	CVE-2016-4573
juniper -- junos	Juniper Junos OS before 12.1X46-D45, 12.1X46-D50, 12.1X47 before 12.1X47-D35, 12.3X48 before 12.3X48-D30, 13.3 before 13.3R9-S1, 14.1 before 14.1R7, 14.2 before 14.2R6, 15.1 before 15.1F2-S5, 15.1F4 before 15.1F4-S2, 15.1R before 15.1R2-S3, 15.1 before 15.1R3, and 15.1X49 before 15.1X49-D40 allow remote attackers to cause a denial of service (kernel crash) via a crafted UDP packet destined to the interface IP address of a 64-bit OS device.	09/09/2016	7.8	CVE-2016-1263
juniper -- junos	Juniper Junos OS before 12.1X46-D50, 12.1X47 before 12.1X47-D40, 12.3X48 before 12.3X48-D30, 13.3 before 13.3R9, 14.1 before 14.1R8, 14.1X53 before 14.1X53-D40, 14.2 before 14.2R6, 15.1 before 15.1F6 or 15.1R3, and 15.1X49 before 15.1X49-D40, when configured with a GRE or IPIP tunnel, allow remote attackers to cause a denial of service (kernel panic) via a crafted ICMP packet.	09/09/2016	7.1	CVE-2016-1277
juniper -- junos	J-Web in Juniper Junos OS before 12.1X46-D45, 12.1X46-D50, 12.1X47 before 12.1X47-D35, 12.3 before 12.3R12, 12.3X48 before 12.3X48-D25, 13.3 before 13.3R10, 13.3R9 before 13.3R9-S1, 14.1 before 14.1R7, 14.1X53 before 14.1X53-D35, 14.2 before 14.2R6, 15.1 before 15.1A2 or 15.1F4, 15.1X49 before 15.1X49-D30, and 15.1R before 15.1R3 might allow remote attackers to obtain sensitive information and consequently gain administrative privileges via unspecified vectors.	09/09/2016	10.0	CVE-2016-1279
hp -- integrated_lights-out_3_firmware	Multiple unspecified vulnerabilities in HPE Integrated Lights-Out 3 (aka iLO 3) firmware before 1.88, Integrated Lights-Out 4 (aka iLO 4) firmware before 2.44, and Integrated Lights-Out 4 (aka iLO 4) mRCA firmware before 2.32 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via unknown vectors.	08/09/2016	7.5	CVE-2016-4375
cracklib_project -- cracklib	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause a denial of service (application crash) or gain privileges via a long GECOS field, involving longbuffer.	07/09/2016	7.2	CVE-2016-6318
f5 -- big-ip_access_policy_manager	F5 BIG-IP LTM, Analytics, APM, ASM, and Link Controller 11.2.x before 11.2.1 HF16, 11.3.x, 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1 HF1, and 12.x before 12.0.0 HF3; BIG-IP AAM, AFM, and PEM 11.4.x, 11.5.x before 11.5.4 HF2, 11.6.x before 11.6.1 HF1, and 12.x before 12.0.0 HF3; BIG-IP DNS 12.x before 12.0.0 HF3; BIG-IP Edge Gateway, WebAccelerator, and WOM 11.2.x before 11.2.1 HF16 and 11.3.0; BIG-IP GTM 11.2.x before 11.2.1 HF16, 11.3.x, 11.4.x, 11.5.x before 11.5.4 HF2, and 11.6.x before 11.6.1 HF1; BIG-IP PSM 11.2.x before 11.2.1 HF16, 11.3.x, and 11.4.0 through 11.4.1; Enterprise Manager 3.1.1; BIG-IQ Cloud and Security 4.0.0 through 4.5.0; BIG-IQ Device 4.2.0 through 4.5.0; BIG-IQ ADC 4.5.0; BIG-IQ Centralized Management 5.0.0; BIG-IQ Cloud and Orchestration 1.0.0; and iWorkflow 2.0.0, when Packet Filtering is enabled on virtual servers and possibly self IP addresses, allow remote attackers to cause a denial of service (Traffic Management Microkernel restart) and possibly have unspecified other impact via crafted network traffic.	07/09/2016	7.5	CVE-2016-5022
huawei -- honor_4c_firmware	The Camera driver in Huawei Honor 4C smartphones with software CHM-UL00C00 before CHM-UL00C00B564, CHM-TL00C01 before CHM-TL00C01B564, and CHM-TL00C00 before CHM-TL00HC00B564 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6180, CVE-2016-6181, CVE-2016-6183, and CVE-2016-6184.	07/09/2016	9.3	CVE-2016-6182
huawei -- uma	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE-2016-7110.	07/09/2016	10.0	CVE-2016-7109
huawei -- uma	Huawei Unified Maintenance Audit (UMA) before V200R001C00SPC200 allows remote attackers to execute arbitrary commands via "special characters," a different vulnerability than CVE-2016-7109.	07/09/2016	10.0	CVE-2016-7110
qemu -- qemu	The esp_do_dma function in hw/scsi/esp.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or execute arbitrary code on the QEMU host via vectors involving DMA read into ESP command buffer.	07/09/2016	7.2	CVE-2016-6351
siemens -- en100_ethernet_module_firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic.	05/09/2016	10.0	CVE-2016-7112
siemens -- en100_ethernet_module_firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets.	05/09/2016	7.8	CVE-2016-7113
siemens -- en100_ethernet_module_firmware	The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to bypass authentication and obtain administrative access via unspecified HTTP traffic during an authenticated session.	05/09/2016	9.0	CVE-2016-7114
cisco -- webex_wrf_player_t29	Cisco WebEx Meetings Player T29.10, when WRF file support is enabled, allows remote attackers to execute arbitrary code via a crafted file, aka Bug ID CSCva09375.	03/09/2016	9.3	CVE-2016-1464
misp-project -- malware_information_sharing_platform	app/Controller/TemplatesController.php in Malware Information Sharing Platform (MISP) before 2.3.92 does not properly restrict filenames under the tmp/files/ directory, which has unspecified impact and attack vectors.	03/09/2016	10.0	CVE-2015-5719
misp-project -- malware_information_sharing_platform	Malware Information Sharing Platform (MISP) before 2.3.90 allows remote attackers to conduct PHP object injection attacks via crafted serialized data, related to TemplatesController.php and populate_event_from_template_attributes.ctp.	03/09/2016	7.5	CVE-2015-5721