Histórico de vulnerabilidades de Xullo do 2016

Semana 25/07/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- unified_computing_system_performance_manager	The web framework in Cisco Unified Computing System (UCS) Performance Manager 2.0.0 and earlier allows remote authenticated users to execute arbitrary commands via crafted parameters in a GET request, aka Bug ID CSCuy07827.	27/07/2016	9.0	CVE-2016-1374
rockwellautomation -- factorytalk_energymetrix	SQL injection vulnerability in Rockwell Automation FactoryTalk EnergyMetrix before 2.20.00 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	27/07/2016	7.5	CVE-2016-4522
rockwellautomation -- factorytalk_energymetrix	Rockwell Automation FactoryTalk EnergyMetrix before 2.20.00 does not invalidate credentials upon a logout action, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.	27/07/2016	7.5	CVE-2016-4531
ca -- ehealth	CA eHealth 6.2.x allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors.	25/07/2016	9.0	CVE-2016-6151
ca -- ehealth	CA eHealth 6.2.x and 6.3.x before 6.3.2.13 allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors.	25/07/2016	9.0	CVE-2016-6152
icu_project -- international_components_for_unicode	The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument.	25/07/2016	7.5	CVE-2016-6293
php -- php	The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.	25/07/2016	7.5	CVE-2016-6288
php -- php	ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.	25/07/2016	7.5	CVE-2016-6290
php -- php	The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.	25/07/2016	7.5	CVE-2016-6291
php -- php	The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.	25/07/2016	7.5	CVE-2016-6294
php -- php	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.	25/07/2016	7.5	CVE-2016-6295
php -- php	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.	25/07/2016	7.5	CVE-2016-6296
google -- chrome	The PPAPI implementation in Google Chrome before 52.0.2743.82 does not validate the origin of IPC messages to the plugin broker process that should have come from the browser process, which allows remote attackers to bypass a sandbox protection mechanism via an unexpected message type, related to broker_process_dispatcher.cc, ppapi_plugin_process_host.cc, ppapi_thread.cc, and render_frame_message_filter.cc.	23/07/2016	9.3	CVE-2016-1706
siemens -- simatic_batch	Siemens SIMATIC WinCC before 7.3 Update 10 and 7.4 before Update 1, SIMATIC BATCH before 8.1 SP1 Update 9 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.1 Update 3 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.2 Update 1 as distributed in SIMATIC PCS 7 8.2, and SIMATIC WinCC Runtime Professional before 13 SP1 Update 9 allow remote attackers to execute arbitrary code via crafted packets.	22/07/2016	10.0	CVE-2016-5743

Semana 18/07/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- retail_integration_bus	Unspecified vulnerability in the Oracle Retail Integration Bus component in Oracle Retail Applications 13.0, 13.1, 13.2, 14.0, 14.1, and 15.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Install.	21/07/2016	10.0	CVE-2016-3444
oracle -- business_intelligence	Unspecified vulnerability in the Oracle Business Intelligence Enterprise Edition component in Oracle Fusion Middleware 11.1.1.7.0 and 11.1.1.9.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Analytics Web Administration.	21/07/2016	7.5	CVE-2016-3446
oracle -- agile_engineering_data_management	Unspecified vulnerability in the Oracle Agile Engineering Data Management component in Oracle Supply Chain Products Suite 6.1.3.0 and 6.2.0.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Install.	21/07/2016	10.0	CVE-2016-3468
oracle -- transportation_management	Unspecified vulnerability in the Oracle Transportation Management component in Oracle Supply Chain Products Suite 6.4.1 allows remote authenticated users to affect confidentiality and integrity via vectors related to Install.	21/07/2016	7.5	CVE-2016-3470
oracle -- mysql	Unspecified vulnerability in Oracle MySQL 5.5.45 and earlier and 5.6.26 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Option.	21/07/2016	7.1	CVE-2016-3471
oracle -- mysql	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.	21/07/2016	7.2	CVE-2016-3477
oracle -- database	Unspecified vulnerability in the Portable Clusterware component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows remote attackers to affect availability via unknown vectors.	21/07/2016	7.8	CVE-2016-3479
oracle -- webcenter_sites	Unspecified vulnerability in the Oracle WebCenter Sites component in Oracle Fusion Middleware 11.1.1.8, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	10.0	CVE-2016-3487
oracle -- database	Unspecified vulnerability in the Data Pump Import component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows local users to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	7.2	CVE-2016-3489
oracle -- crm_technical_foundation	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Wireless Framework.	21/07/2016	8.5	CVE-2016-3491
oracle -- hyperion_financial_reporting	Unspecified vulnerability in the Hyperion Financial Reporting component in Oracle Hyperion 11.1.2.4 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Security Models.	21/07/2016	10.0	CVE-2016-3493
oracle -- weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 12.1.3.0 and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Web Container.	21/07/2016	10.0	CVE-2016-3499
oracle -- weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS Core Components, a different vulnerability than CVE-2016-3586.	21/07/2016	10.0	CVE-2016-3510
oracle -- customer_interaction_history	Unspecified vulnerability in the Oracle Customer Interaction History component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Function Security.	21/07/2016	7.8	CVE-2016-3512
oracle -- enterprise_communications_broker	Unspecified vulnerability in the Oracle Enterprise Communications Broker component in Oracle Communications Applications before PCz 2.0.0m4p1 allows remote attackers to affect confidentiality via unknown vectors.	21/07/2016	7.8	CVE-2016-3515
oracle -- web_applications_desktop_integrator	Unspecified vulnerability in the Oracle Web Applications Desktop Integrator component in Oracle E-Business Suite 12.1.3, 12.2.3, 12.2.4, and 12.2.5 allows remote attackers to affect confidentiality and integrity via vectors related to Application Service.	21/07/2016	8.5	CVE-2016-3522
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality via vectors related to SDK, a different vulnerability than CVE-2016-3529 and CVE-2016-3560.	21/07/2016	7.8	CVE-2016-3526
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to PGC / Import.	21/07/2016	7.5	CVE-2016-3530
oracle -- advanced_inbound_telephony	Unspecified vulnerability in the Oracle Advanced Inbound Telephony component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to SDK client integration.	21/07/2016	7.8	CVE-2016-3532
oracle -- crm_technical_foundation	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Remote Launch.	21/07/2016	7.8	CVE-2016-3535
oracle -- marketing	Unspecified vulnerability in the Oracle Marketing component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Deliverables.	21/07/2016	7.0	CVE-2016-3536
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to File Folders / Attachment, a different vulnerability than CVE-2016-3539.	21/07/2016	7.5	CVE-2016-3538
oracle -- agile_product_lifecycle_management_framework	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to File Folders / Attachment, a different vulnerability than CVE-2016-3538.	21/07/2016	7.5	CVE-2016-3539
oracle -- integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	7.5	CVE-2016-5445
oracle -- integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Infrastructure.	21/07/2016	7.5	CVE-2016-5446
oracle -- integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to IPMI.	21/07/2016	7.5	CVE-2016-5453
oracle -- peoplesoft_enterprise_peopletools	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows local users to affect confidentiality, integrity, and availability via vectors related to Install and Packaging.	21/07/2016	7.2	CVE-2016-5472
harfbuzz_project -- harfbuzz	hb-ot-layout-gpos-table.hh in HarfBuzz before 1.0.5 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data, a different vulnerability than CVE-2016-2052.	19/07/2016	7.5	CVE-2015-8947
misys -- fusioncapital_opics_plus	Misys FusionCapital Opics Plus allows remote authenticated users to gain privileges via a man-in-the-middle attack that modifies the xmlMessaeeOut parameter.	19/07/2016	8.5	CVE-2016-5654
objective_systems -- asn1c	Integer overflow in the rtxMemHeapAlloc function in asn1rt_a.lib in Objective Systems ASN1C for C/C++ before 7.0.2 allows context-dependent attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow), on a system running an application compiled by ASN1C, via crafted ASN.1 data.	19/07/2016	10.0	CVE-2016-5080
ibm -- traveler	IBM Traveler 8.x and 9.x before 9.0.1.12 allows remote authenticated users to read arbitrary files or cause a denial of service (memory consumption) via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.	17/07/2016	8.5	CVE-2016-3039
cisco -- ios_xr	Cisco IOS XR 5.x through 5.2.5 on NCS 6000 devices allows remote attackers to cause a denial of service (timer consumption and Route Processor reload) via crafted SSH traffic, aka Bug ID CSCux76819.	15/07/2016	7.8	CVE-2016-1426
cisco -- ios_xr	The CLI in Cisco IOS XR 6.x through 6.0.1 allows local users to execute arbitrary OS commands in a privileged context by leveraging unspecified container access, aka Bug ID CSCux62721.	15/07/2016	7.2	CVE-2016-1456
hp -- intelligent_management_center_application_performance_manager	HPE iMC PLAT before 7.2 E0403P04, iMC EAD before 7.2 E0405P05, iMC APM before 7.2 E0401P04, iMC NTA before 7.2 E0401P01, iMC BIMS before 7.2 E0402P02, and iMC UAM_TAM before 7.2 E0405P05 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	15/07/2016	7.5	CVE-2016-4372
schneider-electric -- pelco_digital_sentry_video_management_system_firmware	Schneider Electric Pelco Digital Sentry Video Management System with firmware before 7.14 has hardcoded credentials, which allows remote attackers to obtain access, and consequently execute arbitrary code, via unspecified vectors.	15/07/2016	10.0	CVE-2016-4520
schneider-electric -- somachine_hvac_firmware	An unspecified ActiveX control in Schneider Electric SoMachine HVAC Programming Software for M171/M172 Controllers before 2.1.0 allows remote attackers to execute arbitrary code via unknown vectors, related to the INTERFACESAFE_FOR_UNTRUSTED_CALLER (aka safe for scripting) flag.	15/07/2016	7.5	CVE-2016-4529

Histórico de vulnerabilidades de Xullo do 2016

Semana 11/07/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- amqp_0-x_jms_client	Apache Qpid AMQP 0-x JMS client before 6.0.4 and JMS (AMQP 1.0) before 0.10.0 does not restrict the use of classes available on the classpath, which might allow remote attackers to deserialize arbitrary objects and execute arbitrary code by leveraging a crafted serialized object in a JMS ObjectMessage that is handled by the getObject function.	13/07/2016	7.5	CVE-2016-4974
huawei -- hisuite	Huawei HiSuite before 4.0.4.204_ove (Out of China) and before 4.0.4.301 (China) use a weak ACL (FILE_WRITE_DATA for BUILTIN\Users) for the HiSuite service directory, which allows local users to gain SYSTEM privileges via a Trojan horse (1) SspiCli.dll or (2) USERENV.dll file or possibly other unspecified DLL files.	13/07/2016	7.2	CVE-2016-5821
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4172
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4175
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4177.	12/07/2016	10.0	CVE-2016-4176
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4176.	12/07/2016	10.0	CVE-2016-4177
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4179
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4180
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4181
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4182
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4183
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4184
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4185
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4186
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4187
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4188
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4189
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4190
adobe -- acrobat	Integer overflow 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.	12/07/2016	7.5	CVE-2016-4210
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 bypass JavaScript API execution restrictions via unspecified vectors.	12/07/2016	7.5	CVE-2016-4215
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	7.5	CVE-2016-4217
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	7.5	CVE-2016-4218
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	7.5	CVE-2016-4219
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	7.5	CVE-2016-4220
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244. CVE-2016-4245. and CVE-2016-4246.	12/07/2016	7.5	CVE-2016-4221

Histórico de vulnerabilidades de Xullo do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4226
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4227
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4228
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4229
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4231, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4230
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4248.	12/07/2016	10.0	CVE-2016-4231
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4233
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4234
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4235
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4236
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4237
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4238
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4239
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4240
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4241
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4242
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4243
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4245, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4244
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4246.	12/07/2016	10.0	CVE-2016-4245
adobe -- flash_player	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4245.	12/07/2016	10.0	CVE-2016-4246
adobe -- flash_player	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4231.	12/07/2016	10.0	CVE-2016-4248
adobe -- flash_player	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors.	12/07/2016	10.0	CVE-2016-4249
microsoft -- internet_explorer	The Microsoft (1) JScript 5.8 and 9 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3204
microsoft -- windows_10	The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows man-in-the-middle attackers to execute arbitrary code by providing a crafted print driver during printer installation, aka "Windows Print Spooler Remote Code Execution Vulnerability."	12/07/2016	9.3	CVE-2016-3238
microsoft -- windows_10	The Print Spooler service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via vectors involving filesystem write operations, aka "Windows Print Spooler Elevation of Privilege Vulnerability."	12/07/2016	7.2	CVE-2016-3239
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3241 and CVE-2016-3242.	12/07/2016	7.6	CVE-2016-3240
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3242.	12/07/2016	7.6	CVE-2016-3241
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3240 and CVE-2016-3241.	12/07/2016	7.6	CVE-2016-3242
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	12/07/2016	7.6	CVE-2016-3243
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."	12/07/2016	7.6	CVE-2016-3246
microsoft -- edge	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3259.	12/07/2016	9.3	CVE-2016-3248

Histórico de vulnerabilidades de Xullo do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3252, CVE-2016-3254, and CVE-2016-3286.	12/07/2016	7.2	CVE-2016-3249
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Server 2012 and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	12/07/2016	7.2	CVE-2016-3250
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3254, and CVE-2016-3286.	12/07/2016	7.2	CVE-2016-3252
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3286.	12/07/2016	7.2	CVE-2016-3254
microsoft -- edge	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3248.	12/07/2016	9.3	CVE-2016-3259
microsoft -- edge	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3260
microsoft -- edge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	12/07/2016	7.6	CVE-2016-3264
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3269.	12/07/2016	9.3	CVE-2016-3265
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3265.	12/07/2016	9.3	CVE-2016-3269
microsoft -- outlook	Microsoft Outlook 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3278
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3280
microsoft -- office	Microsoft Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3281
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, SharePoint Server 2016, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3282
microsoft -- word_viewer	Microsoft Word Viewer allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3283
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3284
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3254.	12/07/2016	7.2	CVE-2016-3286
linecorp -- line	Untrusted search path vulnerability in LINE and LINE Installer 4.7.0 and earlier on Windows allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	11/07/2016	7.2	CVE-2016-4831
symantec -- client_intrusion_detection_system	The Client Intrusion Detection System (CIDS) driver before 15.0.6 in Symantec Endpoint Protection (SEP) and before 15.1.2 in Norton Security allows remote attackers to cause a denial of service (memory corruption and system crash) via a malformed Portable Executable (PE) file.	11/07/2016	7.1	CVE-2016-5308
google -- android	Unspecified vulnerability in the Qualcomm components in Android before 2016-07-05 allows attackers to gain privileges via a crafted application.	10/07/2016	10.0	CVE-2013-7457
google -- android	The vid_dec_set_meta_buffers function in drivers/video/msm/vidc/common/dec/vdec.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598501 and Qualcomm internal bug CR563654.	10/07/2016	9.3	CVE-2014-9777
google -- android	The vid_dec_set_h264_mv_buffers function in drivers/video/msm/vidc/common/dec/vdec.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598515 and Qualcomm internal bug CR563694.	10/07/2016	9.3	CVE-2014-9778
google -- android	arch/arm/mach-msm/qdsp6v2/msm_audio_ion.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to obtain sensitive information from kernel memory via a crafted offset, aka Android internal bug 28598347 and Qualcomm internal bug CR548679.	10/07/2016	9.3	CVE-2014-9779
google -- android	drivers/video/msm/mdss/mdp3_ctrl.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5, 5X, and 6P devices does not validate start and length values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28602014 and Qualcomm internal bug CR542222.	10/07/2016	9.3	CVE-2014-9780
google -- android	Buffer overflow in drivers/video/fbcmap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28410333 and Qualcomm internal bug CR556471.	10/07/2016	9.3	CVE-2014-9781
google -- android	drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate direction and step parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28431531 and Qualcomm internal bug CR511349.	10/07/2016	9.3	CVE-2014-9782
google -- android	drivers/media/platform/msm/camera_v2/sensor/cci/msm_cci.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate certain values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28441831 and Qualcomm internal bug CR511382.	10/07/2016	9.3	CVE-2014-9783
google -- android	Multiple buffer overflows in drivers/char/diag/diag_debugfs.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28442449 and Qualcomm internal bug CR585147.	10/07/2016	9.3	CVE-2014-9784
google -- android	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate addresses before copying data, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28469042 and Qualcomm internal bug CR545747.	10/07/2016	9.3	CVE-2014-9785
google -- android	Heap-based buffer overflow in drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28557260 and Qualcomm internal bug CR545979.	10/07/2016	9.3	CVE-2014-9786
google -- android	Integer overflow in drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28571496 and Qualcomm internal bug CR545764.	10/07/2016	9.3	CVE-2014-9787
google -- android	Multiple buffer overflows in the voice drivers in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28573112 and Qualcomm internal bug CR548872.	10/07/2016	9.3	CVE-2014-9788
google -- android	The (1) alloc and (2) free APIs in arch/arm/mach-msm/qdsp6v2/msm_audio_ion.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices do not validate parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749392 and Qualcomm internal bug CR556425.	10/07/2016	9.3	CVE-2014-9789
google -- android	drivers/mmc/core/debugfs.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate pointers used in read and write operations, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769136 and Qualcomm internal bug CR545716.	10/07/2016	9.3	CVE-2014-9790
google -- android	arch/arm/mach-msm/ipc_router.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices uses an incorrect integer data type, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769399 and Qualcomm internal bug CR550606.	10/07/2016	9.3	CVE-2014-9792
google -- android	platform/msm_shared/mmc.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices mishandles the power-on write-protect feature, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28821253 and Qualcomm internal bug CR580567.	10/07/2016	9.3	CVE-2014-9793
google -- android	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices does not properly check for an integer overflow, which allows attackers to bypass intended access restrictions via crafted start and size values, aka Android internal bug 28820720 and Qualcomm internal bug CR681957, a related issue to CVE-2014-4325.	10/07/2016	10.0	CVE-2014-9795
google -- android	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the page size in the kernel header, which allows attackers to bypass intended access restrictions via a crafted boot image, aka Android internal bug 28820722 and Qualcomm internal bug CR684756.	10/07/2016	9.3	CVE-2014-9796
google -- android	platform/msm_shared/dev_tree.c in the Qualcomm bootloader in Android before 2016-07-05 on Nexus 5 devices does not check the relationship between tags addresses and aboot addresses, which allows attackers to cause a denial of service (OS outage) via a crafted application, aka Android internal bug 28821448 and Qualcomm internal bug CR681965.	10/07/2016	7.1	CVE-2014-9798
google -- android	The makefile in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices omits the -fno-strict-overflow option to gcc, which might allow attackers to gain privileges via a crafted application that leverages incorrect compiler optimization of an integer-overflow protection mechanism, aka Android internal bug 28821731 and Qualcomm internal bug CR691916.	10/07/2016	9.3	CVE-2014-9799
google -- android	Integer overflow in lib/heap/heap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28822150 and Qualcomm internal bug CR692478.	10/07/2016	9.3	CVE-2014-9800
google -- android	Multiple integer overflows in lib/libfdt/fdt_rw.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28822060 and Qualcomm internal bug CR705078.	10/07/2016	9.3	CVE-2014-9801
google -- android	Multiple integer overflows in lib/libfdt/fdt.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28821965 and Qualcomm internal bug CR705108.	10/07/2016	9.3	CVE-2014-9802
google -- android	arch/arm64/include/asm/pgtable.h in the Linux kernel before 3.15-rc5-next-20140519, as used in Android before 2016-07-05 on Nexus 5X and 6P devices, mishandles execute-only pages, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28557020.	10/07/2016	9.3	CVE-2014-9803
google -- android	Integer overflow in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to bypass intended access restrictions via a crafted block count and block size of a sparse header, aka Android internal bug 28822465 and Qualcomm internal bug CR813933.	10/07/2016	9.3	CVE-2015-8888
google -- android	The aboot implementation in the Qualcomm components in Android before 2016-07-05 on Nexus 6P devices omits the recovery PIN feature, which has unspecified impact and attack vectors, aka Android internal bug 28822677 and Qualcomm internal bug CR804067.	10/07/2016	9.3	CVE-2015-8889
google -- android	platform/msm_shared/partition_parser.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate certain GUID Partition Table (GPT) data, which allows attackers to bypass intended access restrictions via a crafted MultiMediaCard (MMC), aka Android internal bug 28822878 and Qualcomm internal bug CR823461.	10/07/2016	9.3	CVE-2015-8890
google -- android	Multiple integer overflows in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to bypass intended access restrictions via a crafted image, aka Android internal bug 28842418 and Qualcomm internal bug CR813930.	10/07/2016	9.3	CVE-2015-8891
google -- android	platform/msm_shared/boot_verifier.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to bypass intended access restrictions via a digest with trailing data, aka Android internal bug 28822807 and Qualcomm internal bug CR902998.	10/07/2016	9.3	CVE-2015-8892
google -- android	drivers/gpu/msm/kgsl.c in the MSM graphics driver (aka GPU driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, mishandles the KGSL_MEMFLAGS_GPUREADONLY flag, which allows attackers to gain privileges by leveraging accidental read-write mappings, aka Qualcomm internal bug CR888993.	10/07/2016	9.3	CVE-2016-2067

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	The MSM QDSP6 audio driver (aka sound driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (integer overflow, and buffer overflow or buffer over-read) via a crafted application that performs a (1) AUDIO_EFFECTS_WRITE or (2) AUDIO_EFFECTS_READ operation, aka Qualcomm internal bug CR1006609.	10/07/2016	9.3	CVE-2016-2068
google -- android	The Qualcomm camera driver in Android before 2016-07-05 on Nexus 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 27890722 and Qualcomm internal bug CR1001092.	10/07/2016	9.3	CVE-2016-2501
google -- android	drivers/usb/gadget/f_serial.c in the Qualcomm USB driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a large size in a GSER_IOCTL ioctl call, aka Android internal bug 27657963 and Qualcomm internal bug CR997044.	10/07/2016	9.3	CVE-2016-2502
google -- android	The Qualcomm GPU driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28084795 and Qualcomm internal bug CR1006067.	10/07/2016	9.3	CVE-2016-2503
google -- android	mpeg2ts/ATSParser.cpp in libstagefright in mediaserver in Android 6.x before 2016-07-01 does not validate a certain section length, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28333006.	10/07/2016	9.3	CVE-2016-2505
google -- android	DRMExtractor.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 2016-07-01 does not validate a certain offset value, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28175045.	10/07/2016	10.0	CVE-2016-2506
google -- android	Integer overflow in codecs/on2/h264dec/source/h264bsd_storage.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 2016-07-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28532266.	10/07/2016	9.3	CVE-2016-2507
google -- android	media/libmediaplayerservice/nuplayer/GenericSource.cpp in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate certain track data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28799341.	10/07/2016	9.3	CVE-2016-2508
google -- android	The H.264 decoder in mediaserver in Android 6.x before 2016-07-01 does not initialize certain slice data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28165661.	10/07/2016	7.5	CVE-2016-3741
google -- android	decoder/ih264d_process_intra_mb.c in mediaserver in Android 6.x before 2016-07-01 mishandles intra mode, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28165659.	10/07/2016	7.5	CVE-2016-3742
google -- android	decoder/ih264d_api.c in mediaserver in Android 6.x before 2016-07-01 does not initialize certain data structures, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 27907656.	10/07/2016	7.5	CVE-2016-3743
google -- android	Multiple buffer overflows in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allow attackers to gain privileges via a crafted application that provides an AudioEffect reply, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 28173666.	10/07/2016	7.5	CVE-2016-3745
google -- android	Use-after-free vulnerability in the mm-video-v4l2 vdec component in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27890802.	10/07/2016	7.5	CVE-2016-3746
google -- android	Use-after-free vulnerability in the mm-video-v4l2 venc component in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27903498.	10/07/2016	10.0	CVE-2016-3747
google -- android	The sockets subsystem in Android 6.x before 2016-07-01 allows attackers to bypass intended system-call restrictions via a crafted application that makes an ioctl call, aka internal bug 28171804.	10/07/2016	7.5	CVE-2016-3748
google -- android	libs/binder/Parcel.cpp in the Parcels Framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate the return value of the dup system call, which allows attackers to bypass an isolation protection mechanism via a crafted application, aka internal bug 28395952.	10/07/2016	7.5	CVE-2016-3750
google -- android	internal/app/ChooserActivity.java in the ChooserTarget service in Android 6.x before 2016-07-01 mishandles target security checks, which allows attackers to gain privileges via a crafted application, aka internal bug 28384423.	10/07/2016	7.5	CVE-2016-3752
google -- android	mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not limit process-memory usage, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28615448.	10/07/2016	7.8	CVE-2016-3754
google -- android	decoder/ih264d_parse_pslice.c in mediaserver in Android 6.x before 2016-07-01 does not properly select concealment frames, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28470138.	10/07/2016	7.8	CVE-2016-3755
google -- android	Tremolo/res012.c in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate the number of partitions, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28556125.	10/07/2016	7.8	CVE-2016-3756
google -- android	Multiple buffer overflows in libdex/OptInvocation.cpp in DexClassLoader in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allow attackers to gain privileges via a crafted application that provides a long filename, aka internal bug 27840771.	10/07/2016	9.3	CVE-2016-3758
google -- android	The sockets subsystem in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application that uses (1) the AF_MSM_IPC socket class or (2) another socket class that is unrecognized by SELinux, aka internal bug 28612709.	10/07/2016	9.3	CVE-2016-3762
google -- android	MPEG4Extractor.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 2016-07-01 does not check whether memory allocation succeeds, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28471206.	10/07/2016	7.8	CVE-2016-3766
google -- android	The MediaTek Wi-Fi driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28169363 and MediaTek internal bug ALPS02689526.	10/07/2016	9.3	CVE-2016-3767
google -- android	The Qualcomm performance component in Android before 2016-07-05 on Nexus 5, 6, 5X, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28172137 and Qualcomm internal bug CR1010644.	10/07/2016	9.3	CVE-2016-3768
google -- android	The NVIDIA video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28376656.	10/07/2016	9.3	CVE-2016-3769
google -- android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28346752 and MediaTek internal bug ALPS02703102.	10/07/2016	9.3	CVE-2016-3770
google -- android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29007611 and MediaTek internal bug ALPS02703102.	10/07/2016	9.3	CVE-2016-3771
google -- android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008188 and MediaTek internal bug ALPS02703102.	10/07/2016	9.3	CVE-2016-3772
google -- android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008363 and MediaTek internal bug ALPS02703102.	10/07/2016	9.3	CVE-2016-3773
google -- android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application, aka Android internal bug 29008609 and MediaTek internal bug ALPS02703102.	10/07/2016	9.3	CVE-2016-3774
google -- android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28588279.	10/07/2016	9.3	CVE-2016-3775
google -- android	CORE/HDD/src/wlan_hdd_hostapd.c in the Qualcomm Wi-Fi driver in Android before 2016-07-05 on Nexus 7 (2013) devices mishandles userspace data copying, which allows attackers to gain privileges via a crafted application, aka Android internal bug 27725204 and Qualcomm internal bug CR561022.	10/07/2016	9.3	CVE-2016-3792
google -- android	The NVIDIA camera driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28026625.	10/07/2016	9.3	CVE-2016-3793
google -- android	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28085222 and MediaTek internal bug ALPS02677244.	10/07/2016	9.3	CVE-2016-3795
google -- android	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 29008443 and MediaTek internal bug ALPS02677244.	10/07/2016	9.3	CVE-2016-3796
google -- android	The Qualcomm Wi-Fi driver in Android before 2016-07-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28085680 and Qualcomm internal bug CR1001450.	10/07/2016	9.3	CVE-2016-3797
google -- android	The MediaTek hardware sensor driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28174490 and MediaTek internal bug ALPS02703105.	10/07/2016	9.3	CVE-2016-3798
google -- android	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28175025 and MediaTek internal bug ALPS02693738.	10/07/2016	9.3	CVE-2016-3799
google -- android	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28175027 and MediaTek internal bug ALPS02693739.	10/07/2016	9.3	CVE-2016-3800
google -- android	The MediaTek GPS driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28174914 and MediaTek internal bug ALPS02688853.	10/07/2016	9.3	CVE-2016-3801
google -- android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28271368.	10/07/2016	9.3	CVE-2016-3802
google -- android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 28588434.	10/07/2016	9.3	CVE-2016-3803
google -- android	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28332766 and MediaTek internal bug ALPS02694410.	10/07/2016	9.3	CVE-2016-3804
google -- android	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28333002 and MediaTek internal bug ALPS02694412.	10/07/2016	9.3	CVE-2016-3805
google -- android	The MediaTek display driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28402341 and MediaTek internal bug ALPS02715341.	10/07/2016	9.3	CVE-2016-3806
google -- android	The serial peripheral interface driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 28402196.	10/07/2016	9.3	CVE-2016-3807
google -- android	The serial peripheral interface driver in Android before 2016-07-05 on Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28430009.	10/07/2016	9.3	CVE-2016-3808
google -- android	The kernel video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28447556.	10/07/2016	9.3	CVE-2016-3811
google -- android	libc in Android 4.x before 4.4.4 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28740702.	10/07/2016	7.1	CVE-2016-3818
libpng -- libpng	Unspecified vulnerability in libpng before 1.6.20, as used in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01, allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 23265085.	10/07/2016	7.5	CVE-2016-3751

Semana 04/07/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- commons_fileupload	The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.	04/07/2016	7.8	CVE-2016-3092
apache -- struts	The REST plugin in Apache Struts 2 2.3.20 through 2.3.28.1 allows remote attackers to execute arbitrary code via a crafted expression.	04/07/2016	7.5	CVE-2016-4438
apple -- airport_base_station_firmware	Apple AirPort Base Station Firmware before 7.6.7 and 7.7.x before 7.7.7 misparses DNS data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	02/07/2016	10.0	CVE-2015-7029
cisco -- evolved_programmable_network_manager	The API in Cisco Prime Infrastructure 1.2 through 3.0 and Evolved Programmable Network Manager (EPNM) 1.2 allows remote attackers to execute arbitrary code or obtain sensitive management information via a crafted HTTP request, as demonstrated by discovering managed-device credentials, aka Bug ID CSCuy10231.	02/07/2016	10.0	CVE-2016-1289
cisco -- epc3928_firmware	goform/WClientMACList on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long h_sortWireless parameter, related to a "Gateway Client List Denial of Service" issue, aka Bug ID CSCux24948.	03/07/2016	7.8	CVE-2016-1328
cisco -- epc3928_firmware	goform/Docsis_system on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long LanguageSelect parameter, related to a "Gateway HTTP Corruption Denial of Service" issue, aka Bug ID CSCuy28100.	03/07/2016	7.8	CVE-2016-1336
cisco -- firesight_system_software	Cisco Firepower System Software 6.0.0 through 6.1.0 has a hardcoded account, which allows remote attackers to obtain CLI access by leveraging knowledge of the password, aka Bug ID CSCux56238.	02/07/2016	7.5	CVE-2016-1394
cisco -- prime_collaboration_provisioning	Cisco Prime Collaboration Provisioning 10.6 SP2 (aka 10.6.0.10602) mishandles LDAP authentication, which allows remote attackers to obtain administrator privileges via a crafted login attempt, aka Bug ID CSCuv37513.	02/07/2016	10.0	CVE-2016-1416
cisco -- prime_infrastructure	The administrative web interface in Cisco Prime Infrastructure (PI) before 3.1.1 allows remote authenticated users to execute arbitrary commands via crafted field values, aka Bug ID CSCuy96280.	07/07/2016	9.0	CVE-2016-1442
eaton -- elcsoft	Stack-based buffer overflow in ELCSimulator in Eaton ELCSoft 2.4.01 and earlier allows remote attackers to execute arbitrary code via a long packet.	03/07/2016	7.5	CVE-2016-4512
ibm -- power_hardware_management_console	IBM Power Hardware Management Console (HMC) 7.3 through 7.3.0 SP7, 7.9 through 7.9.0 SP3, 8.1 through 8.1.0 SP3, 8.2 through 8.2.0 SP2, 8.3 through 8.3.0 SP2, 8.4 through 8.4.0 SP1, and 8.5.0 allows physically proximate attackers to obtain root access via unspecified vectors.	07/07/2016	7.2	CVE-2016-0230
ibm -- urbancode_deploy	The agents in IBM UrbanCode Deploy 6.x before 6.0.1.14, 6.1.x before 6.1.3.3, and 6.2.x before 6.2.1.1 do not verify a server's identity in a JMS session or an HTTP session, which allows local users to obtain root access to arbitrary agents via unspecified vectors.	07/07/2016	7.2	CVE-2016-0271
ibm -- watson_developer_cloud	The IBM Watson Developer Cloud services on Bluemix platforms do not properly generate random numbers for service-instance credentials, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.	02/07/2016	7.5	CVE-2016-0391
linux -- linux_kernel	The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted length value in a USB/IP packet.	03/07/2016	10.0	CVE-2016-3955
linux -- linux_kernel	The compat IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.	03/07/2016	7.2	CVE-2016-4997
meinberg -- ims-lantime_m1000	Stack-based buffer overflow in the NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request.	03/07/2016	7.5	CVE-2016-3962
meinberg -- ims-lantime_m1000	Multiple stack-based buffer overflows in the NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request.	03/07/2016	7.5	CVE-2016-3988
meinberg -- ims-lantime_m1000	The NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote authenticated users to obtain root privileges for writing to unspecified scripts, and consequently obtain sensitive information or modify data, by leveraging access to the nobody account.	03/07/2016	8.5	CVE-2016-3989
microfocus -- rumba	Multiple stack-based buffer overflows in COM objects in Micro Focus Rumba 9.4.x before 9.4 HF 13960 allow remote attackers to execute arbitrary code via (1) the NetworkName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (2) the CPName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (3) the PrinterName property value to ProfileEditor.PrintPasteControl in ProfEdit.dll, (4) the Data argument to the WriteRecords function in FTXBIFFLib.AS400FtxBIFF in FtxBIFF.dll, (5) the Serialized property value to NMSECCOMPARAMSLib.SSL3 in NMSecComParams.dll, (6) the UserName property value to NMSECCOMPARAMSLib.FirewallProxy in NMSecComParams.dll, (7) the LUName property value to ProfileEditor.MFSNAControl in ProfEdit.dll, (8) the newVal argument to the Load function in FTPSFTPLib.SFtpSession in FTPSFtp.dll, or (9) a long Host field in the FTP Client.	02/07/2016	10.0	CVE-2016-1606
microfocus -- rumba	Stack-based buffer overflow in the PlayMacro function in ObjectXMacro.ObjectXMacro in WdMacCtl.ocx in Micro Focus Rumba 9.x before 9.3 HF 11997 and 9.4.x before 9.4 HF 12815 allows remote attackers to execute arbitrary code via a long MacroName argument. NOTE: some references mention CVE-2016-5226 but that is not a correct ID for any Rumba vulnerability.	02/07/2016	10.0	CVE-2016-5228
openvswitch -- openvswitch	Buffer overflow in lib/flow.c in ovs-vswitchd in Open vSwitch 2.2.x and 2.3.x before 2.3.3 and 2.4.x before 2.4.1 allows remote attackers to execute arbitrary code via crafted MPLS packets, as demonstrated by a long string in an ovs-appctl command.	03/07/2016	7.5	CVE-2016-2074
phpmyadmin -- phpmyadmin	SQL injection vulnerability in libraries/central_columns.lib.php in phpMyAdmin 4.4.x before 4.4.15.7 and 4.6.x before 4.6.3 allows remote attackers to execute arbitrary SQL commands via a crafted database name that is mishandled in a central column query.	02/07/2016	7.5	CVE-2016-5703
phpmyadmin -- phpmyadmin	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not properly choose delimiters to prevent use of the preg_replace e (aka eval) modifier, which might allow remote attackers to execute arbitrary PHP code via a crafted string, as demonstrated by the table search-and-replace implementation.	02/07/2016	7.5	CVE-2016-5734