Histórico de vulnerabilidades de Noviembre del 2015

Semana 23/11/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
csl_dualcom -- gprs_cs2300-r_firmware	CSL DualCom GPRS CS2300-R devices with firmware 1.25 through 3.53 use the same 001984 default PIN across different customers' installations, which allows remote attackers to execute commands by leveraging knowledge of this PIN and including it in an SMS message.	24/11/2015	7.5	CVE-2015-7287
gnome -- gnome_display_manager	GNOME Display Manager (gdm) before 3.18.2 allows physically proximate attackers to bypass the lock screen by holding the Escape key.	24/11/2015	7.2	CVE-2015-7496
huawei -- vp_9660_firmware	The built-in web server in Huawei VP9660 multi-point control unit with software before V200R001C30SPC700 allows a remote administrator to obtain sensitive information or cause a denial of service via a crafted message.	24/11/2015	8.5	CVE-2015-8227
nvidia -- gpu_driver	The host memory mapping path feature in the NVIDIA GPU graphics driver R346 before 346.87 and R352 before 352.41 for Linux and R352 before 352.46 for GRID vGPU and vSGA does not properly restrict access to third-party device IO memory, which allows attackers to gain privileges, cause a denial of service (resource consumption), or possibly have unspecified other impact via unknown vectors related to the follow_pfn kernel-mode API call.	24/11/2015	10.0	CVE-2015-5053
nvidia -- gpu_driver	nvSCPAPISvr.exe in the Stereoscopic 3D Driver Service in the NVIDIA GPU graphics driver R340 before 341.92, R352 before 354.35, and R358 before 358.87 on Windows does not properly restrict access to the stereosvrpipe named pipe, which allows local users to gain privileges via a commandline in a number 2 command, which is stored in the HKEY_LOCAL_MACHINE explorer Run registry key, a different vulnerability than CVE-2011-4784.	24/11/2015	7.7	CVE-2015-7865
nvidia -- gpu_driver	Unquoted Windows search path vulnerability in the Smart Maximize Helper (nvSmartMaxApp.exe) in the Control Panel in the NVIDIA GPU graphics driver R340 before 341.92, R352 before 354.35, and R358 before 358.87 on Windows allows local users to gain privileges via a Trojan horse application, as demonstrated by C:\Program.exe.	24/11/2015	7.2	CVE-2015-7866
sap -- plant_connectivity	The PCo agent in SAP Plant Connectivity (PCo) allows remote attackers to cause a denial of service (memory corruption and agent crash) via crafted xMII requests, aka SAP Security Note 2238619.	24/11/2015	7.8	CVE-2015-8330
valve -- steam	Valve Steam 2.10.91.91 uses weak permissions (Users: read and write) for the Install folder, which allows local users to gain privileges via a Trojan horse steam.exe file.	24/11/2015	7.2	CVE-2015-7985
vbulletin -- vbulletin	The vB_Api_Hook::decodeArguments method in vBulletin 5 Connect 5.1.2 through 5.1.9 allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted serialized object in the arguments parameter to ajax/api/hook/decodeArguments.	24/11/2015	7.5	CVE-2015-7808
cisco -- virtual_topology_system	Cisco Virtual Topology System (VTS) 2.0(0) and 2.0(1) allows remote attackers to cause a denial of service (CPU and memory consumption, and TCP port outage) via a flood of crafted TCP packets, aka Bug ID CSCux13379.	23/11/2015	7.8	CVE-2015-6377
apple -- iphone_os	The fts3_tokenizer function in SQLite, as used in Apple iOS before 8.4 and OS X before 10.10.4, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a SQL command that triggers an API call with a crafted pointer value in the second argument.	21/11/2015	7.5	CVE-2015-7036
arris -- na_model_862_gw_mono_firmware	Arris DG860A, TG862A, and TG862G devices with firmware TS0703128_100611 through TS0705125D_031115 have a hardcoded administrator password derived from a serial number, which makes it easier for remote attackers to obtain access via the web management interface, SSH, TELNET, or SNMP.	21/11/2015	9.3	CVE-2015-7289
tibbo -- aggregate	The Ice Faces servlet in ag_server_service.exe in the AggreGate Server Service in Tibbo AggreGate before 5.30.06 allows remote attackers to upload and execute arbitrary Java code via a crafted XML document.	21/11/2015	10.0	CVE-2015-7912
tibbo -- aggregate	ag_server_service.exe in the AggreGate Server Service in Tibbo AggreGate before 5.30.06 allows local users to execute arbitrary Java code with SYSTEM privileges by using the Apache Axis AdminService deployment method to publish a class.	21/11/2015	7.2	CVE-2015-7913

Semana 16/11/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arista -- eos	Arista EOS before 4.11.12, 4.12 before 4.12.11, 4.13 before 4.13.14M, 4.14 before 4.14.5FX.5, and 4.15 before 4.15.0FX1.1 allows remote attackers to execute arbitrary code as root by leveraging management-plane access, aka Bug 138716.	19/11/2015	10.0	CVE-2015-8236
dracut_project -- dracut	modules.d/90crypt/module-setup.sh in the dracut package before 037-17.30.1 in openSUSE 13.2 allows local users to have unspecified impact via a symlink attack on /tmp/dracut_block_uuid.map.	19/11/2015	7.2	CVE-2015-0794
exemys -- telemetry_web_server	Exemys Telemetry Web Server relies on an HTTP Location header to indicate that a client is unauthorized, which allows remote attackers to bypass intended access restrictions by disregarding this header and processing the response body.	19/11/2015	7.8	CVE-2015-7910
huawei -- espace_firmware	An unspecified module in Huawei eSpace U1910, U1911, U1930, U1960, U1980, and U1981 unified gateways with software before V200R003C00SPC300 does not properly initialize memory when processing timeout messages, which allows remote attackers to cause a denial of service (out-of-bounds memory access and device restart) via unknown vectors.	19/11/2015	7.8	CVE-2015-8083
adobe -- premiere_clip	The Adobe Premiere Clip app before 1.2.1 for iOS mishandles unspecified input, which has unknown impact and attack vectors.	18/11/2015	10.0	CVE-2015-8051
cisco -- firepower_extensible_operating_system	The Management I/O (MIO) component in Cisco Firepower Extensible Operating System 1.1(1.160) on Firepower 9000 devices allows local users to execute arbitrary OS commands as root via crafted CLI input, aka Bug ID CSCux10578.	18/11/2015	7.2	CVE-2015-6370
oracle -- weblogic_server	The WLS Security component in Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to execute arbitrary commands via a crafted serialized Java object in T3 protocol traffic to TCP port 7001, related to oracle_common/modules/com.bea.core.apache.commons.collections.jar. NOTE: the scope of this CVE is limited to the WebLogic Server product.	18/11/2015	7.5	CVE-2015-4852
dameware -- mini_remote_control	Stack-based buffer overflow in the URI handler in DWRCC.exe in SolarWinds DameWare Mini Remote Control before 12.0 HotFix 1 allows remote attackers to execute arbitrary code via a crafted commandline argument in a link.	17/11/2015	7.5	CVE-2015-8220
google -- picasa	Integer overflow in Google Picasa before 3.9.140 Build 259 allows remote attackers to execute arbitrary code via the CAMF section in a FOVb image, which triggers a heap-based buffer overflow.	17/11/2015	10.0	CVE-2015-8221
mega-nerd -- libsndfile	Heap-based buffer overflow in libsndfile 1.0.25 allows remote attackers to have unspecified impact via the headindex value in the header in an AIFF file.	17/11/2015	9.3	CVE-2015-7805
sudo_project -- sudo	sudoedit in Sudo before 1.8.15 allows local users to gain privileges via a symlink attack on a file whose full path is defined using multiple wildcards in /etc/sudoers, as demonstrated by "/home/*/*/file.txt."	17/11/2015	7.2	CVE-2015-5602
ffmpeg -- ffmpeg	The ljpeg_decode_yuv_scan function in libavcodec/mjpegdec.c in FFmpeg before 2.8.2 omits certain width and height checks, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted MJPEG data.	16/11/2015	7.5	CVE-2015-8216
ffmpeg -- ffmpeg	The ff_hevc_parse_sps function in libavcodec/hevc_ps.c in FFmpeg before 2.8.2 does not validate the Chroma Format Indicator, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted High Efficiency Video Coding (HEVC) data.	16/11/2015	7.5	CVE-2015-8217
ffmpeg -- ffmpeg	The init_tile function in libavcodec/jpeg2000dec.c in FFmpeg before 2.8.2 does not enforce minimum-value and maximum-value constraints on tile coordinates, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data.	16/11/2015	7.5	CVE-2015-8219
piwik -- piwik	Directory traversal vulnerability in core/ViewDataTable/Factory.php in Piwik before 2.15.0 allows remote attackers to include and execute arbitrary local files via the viewDataTable parameter.	16/11/2015	7.5	CVE-2015-7815
piwik -- piwik	The DisplayTopKeywords function in plugins/Referrers/Controller.php in Piwik before 2.15.0, which allows remote attackers to conduct PHP object injection attacks, conduct Server-Side Request Forgery (SSRF) attacks, and execute arbitrary PHP code via a crafted HTTP header.	16/11/2015	7.5	CVE-2015-7816
samsung -- galaxy_s6	The media scanning functionality in the face recognition library in android.media.process in Samsung Galaxy S6 Edge before G925VVRU4B0G9 allows remote attackers to gain privileges or cause a denial of service (memory corruption) via a crafted BMP image file.	16/11/2015	7.5	CVE-2015-7897
schneider-electric -- imt25_magnetic_flow_dtm	Buffer overflow in Schneider Electric IMT25 Magnetic Flow DTM before 1.500.004 for the HART Protocol allows remote authenticated users to execute arbitrary code or cause a denial of service (memory corruption) via a crafted HART reply.	14/11/2015	7.7	CVE-2015-3977
cisco -- aironet_access_point_software	Cisco Aironet 1800 devices with software 8.1(131.0) allow remote attackers to cause a denial of service (CPU consumption) by improperly establishing many SSHv2 connections, aka Bug ID CSCux13374.	13/11/2015	7.8	CVE-2015-6367
ibm -- websphere_portal	IBM WebSphere Portal 8.0.0.1 before CF19 and 8.5.0 before CF09 allows remote attackers to cause a denial of service (memory consumption) via crafted requests.	13/11/2015	7.8	CVE-2015-7419

Semana 09/11/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libpng -- libpng	Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.	12/11/2015	7.5	CVE-2015-8126
microsoft -- internet_explorer	Use-after-free vulnerability in the CElement object implementation in Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JavaScript that improperly interacts with use of the Cascading Style Sheets (CSS) empty-cells property for a TABLE element, aka "Internet Explorer Memory Corruption Vulnerability."	12/11/2015	9.3	CVE-2015-6045
mit -- kerberos	The iakerb_gss_export_sec_context function in lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) 1.14 pre-release 2015-09-14 improperly accesses a certain pointer, which allows remote authenticated users to cause a denial of service (memory corruption) or possibly have unspecified other impact by interacting with an application that calls the gss_export_sec_context function. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-2696.	12/11/2015	8.5	CVE-2015-2698
unitronics -- visilogic_oplc_ide	Unitronics VisiLogic OPLC IDE before 9.8.02 allows remote attackers to execute unspecified code via unknown vectors.	12/11/2015	7.5	CVE-2015-7905
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted DefineFunction atoms, a different vulnerability than CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7651
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted gridFitType property value, a different vulnerability than CVE-2015-7651, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7652
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted globalToLocal arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7653
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted attachSound arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7654
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionExtends arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7655
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionImplementsOp arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7656
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionCallMethod arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7657
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionInstanceOf arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7658
adobe -- air	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion" in the NetConnection object implementation.	11/11/2015	9.3	CVE-2015-7659
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted setMask arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7660
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted getBounds call, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-7661
adobe -- air	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow remote attackers to bypass intended access restrictions and write to files via unspecified vectors.	11/11/2015	7.8	CVE-2015-7662
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	10.0	CVE-2015-7663
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted loadSound call, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	9.3	CVE-2015-8042
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8044, and CVE-2015-8046.	11/11/2015	10.0	CVE-2015-8043
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, and CVE-2015-8046.	11/11/2015	10.0	CVE-2015-8044
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, and CVE-2015-8044.	11/11/2015	10.0	CVE-2015-8046
google -- chrome	The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.	11/11/2015	7.5	CVE-2015-1302
ibm -- system_networking_switch_center	Race condition in the administration-panel web service in IBM System Networking Switch Center (SNSC) before 7.3.1.5 and Lenovo Switch Center before 8.1.2.0 allows remote attackers to obtain privileged-account access, and consequently provide FileReader.jsp input containing directory traversal sequences to read arbitrary text files, via a request to port 40080 or 40443.	11/11/2015	7.1	CVE-2015-7817
ibm -- system_networking_switch_center	The administration-panel web service in IBM System Networking Switch Center (SNSC) before 7.3.1.5 and Lenovo Switch Center before 8.1.2.0 allows local users to execute arbitrary JSP code with SYSTEM privileges by using the Apache Axis AdminService deployment method to install a .jsp file.	11/11/2015	7.2	CVE-2015-7818
ibm -- system_networking_switch_center	Race condition in the administration-panel web service in IBM System Networking Switch Center (SNSC) before 7.3.1.5 and Lenovo Switch Center before 8.1.2.0 allows remote attackers to obtain privileged-account access, and consequently provide ZipDownload.jsp input containing directory traversal sequences to read arbitrary files, via a request to port 40080 or 40443.	11/11/2015	7.1	CVE-2015-7820
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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."	11/11/2015	9.3	CVE-2015-2427
microsoft -- windows_10	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application that triggers a Winsock call referencing an invalid address, aka "Winsock Elevation of Privilege Vulnerability."	11/11/2015	7.2	CVE-2015-2478
microsoft -- access	Microsoft Access 2007 SP3, Excel 2007 SP3, InfoPath 2007 SP3, OneNote 2007 SP3, PowerPoint 2007 SP3, Project 2007 SP3, Publisher 2007 SP3, Visio 2007 SP3, Word 2007 SP3, Office 2007 IME (Japanese) SP3, Access 2010 SP2, Excel 2010 SP2, InfoPath 2010 SP2, OneNote 2010 SP2, PowerPoint 2010 SP2, Project 2010 SP2, Publisher 2010 SP2, Visio 2010 SP2, Word 2010 SP2, Pinyin IME 2010, Access 2013 SP1, Excel 2013 SP1, InfoPath 2013 SP1, OneNote 2013 SP1, PowerPoint 2013 SP1, Project 2013 SP1, Publisher 2013 SP1, Visio 2013 SP1, Word 2013 SP1, Excel 2013 RT SP1, OneNote 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Access 2016, Excel 2016, OneNote 2016, PowerPoint 2016, Project 2016, Publisher 2016, Visio 2016, Word 2016, Skype for Business 2016, and Lync 2013 SP1 allow remote attackers to bypass a sandbox protection mechanism and gain privileges via a crafted web site that is accessed with Internet Explorer, as demonstrated by a transition from Low Integrity to Medium Integrity, aka "Microsoft Office Elevation of Privilege Vulnerability."	11/11/2015	9.3	CVE-2015-2503
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, Excel Viewer, and Excel Services on SharePoint Server 2007 SP3, 2010 SP2, and 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	11/11/2015	9.3	CVE-2015-6038
microsoft -- edge	Microsoft Internet Explorer 10 and 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," a different vulnerability than CVE-2015-6084 and CVE-2015-6085.	11/11/2015	9.3	CVE-2015-6064
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-2015-6078.	11/11/2015	9.3	CVE-2015-6065
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6070, CVE-2015-6071, CVE-2015-6074, CVE-2015-6076, and CVE-2015-6087.	11/11/2015	9.3	CVE-2015-6066

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6068
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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-2015-6081.	11/11/2015	9.3	CVE-2015-6069
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6066, CVE-2015-6071, CVE-2015-6074, CVE-2015-6076, and CVE-2015-6087.	11/11/2015	9.3	CVE-2015-6070
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6066, CVE-2015-6070, CVE-2015-6074, CVE-2015-6076, and CVE-2015-6087.	11/11/2015	9.3	CVE-2015-6071
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6072
microsoft -- edge	Microsoft Internet Explorer 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," a different vulnerability than CVE-2015-6068, CVE-2015-6072, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6073
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015-6076, and CVE-2015-6087.	11/11/2015	9.3	CVE-2015-6074
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6077, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6075
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015-6074, and CVE-2015-6087.	11/11/2015	9.3	CVE-2015-6076
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6079, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6077
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," a different vulnerability than CVE-2015-6065.	11/11/2015	9.3	CVE-2015-6078
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6080, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6079
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, and CVE-2015-6082.	11/11/2015	9.3	CVE-2015-6080
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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-2015-6069.	11/11/2015	9.3	CVE-2015-6081
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2015-6068, CVE-2015-6072, CVE-2015-6073, CVE-2015-6075, CVE-2015-6077, CVE-2015-6079, and CVE-2015-6080.	11/11/2015	9.3	CVE-2015-6082
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," a different vulnerability than CVE-2015-6064 and CVE-2015-6085.	11/11/2015	9.3	CVE-2015-6084
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," a different vulnerability than CVE-2015-6064 and CVE-2015-6084.	11/11/2015	9.3	CVE-2015-6085
microsoft -- internet_explorer	Microsoft Internet Explorer 7 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-2015-6066, CVE-2015-6070, CVE-2015-6071, CVE-2015-6074, and CVE-2015-6076.	11/11/2015	9.3	CVE-2015-6087
microsoft -- jscript	The Microsoft (1) VBScript and (2) JScript engines, as used in Internet Explorer 8 through 11, 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."	11/11/2015	9.3	CVE-2015-6089
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	11/11/2015	9.3	CVE-2015-6091
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, 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."	11/11/2015	9.3	CVE-2015-6092
microsoft -- office	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office 2016, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, Office Web Apps 2010 SP2, and Office Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	11/11/2015	9.3	CVE-2015-6093
microsoft -- excel	Microsoft Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, and Excel Services on SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	11/11/2015	9.3	CVE-2015-6094
microsoft -- windows_7	Heap-based buffer overflow in Windows Journal in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted Journal (.jnt) file, aka "Windows Journal Heap Overflow Vulnerability."	11/11/2015	9.3	CVE-2015-6097
microsoft -- windows_7	Buffer overflow in the Network Driver Interface Standard (NDIS) implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka "Windows NDIS Elevation of Privilege Vulnerability."	11/11/2015	7.2	CVE-2015-6098
microsoft -- windows_10	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6101.	11/11/2015	7.2	CVE-2015-6100
microsoft -- windows_10	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6100.	11/11/2015	7.2	CVE-2015-6101
microsoft -- windows_10	The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-6104.	11/11/2015	9.3	CVE-2015-6103
microsoft -- windows_10	The Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-6103.	11/11/2015	9.3	CVE-2015-6104
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM) 12.1 before 12.1-RU6-MP3 allows remote attackers to execute arbitrary OS commands via crafted data.	11/11/2015	7.5	CVE-2015-6554
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM) 12.1 before 12.1-RU6-MP3 allows remote attackers to execute arbitrary Java code by connecting to the console Java port.	11/11/2015	8.5	CVE-2015-6555
symantec -- endpoint_protection	Untrusted search path vulnerability in the client in Symantec Endpoint Protection (SEP) 12.1 before 12.1-RU6-MP3 allows local users to gain privileges via a Trojan horse DLL in a client install package. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1492.	11/11/2015	7.2	CVE-2015-8113
sap -- hana	SAP HANA Database 1.00 SPS10 and earlier do not require authentication, which allows remote attackers to execute arbitrary code or have unspecified other impact via a TrexNet packet to the (1) fcopydir, (2) fmkdir, (3) frmdir, (4) getenv, (5) dumpenv, (6) fcopy, (7) fput, (8) fdel, (9) fmove, (10) fget, (11) fappend, (12) fdir, (13) getTraces, (14) kill, (15) pexec, (16) stop, or (17) pythonexec method, aka SAP Security Note 2165583.	10/11/2015	10.0	CVE-2015-7828
sap -- hana	The Extended Application Services (aka XS or XS Engine) in SAP HANA DB 1.00.73.00.389160 (NewDB100_REL) allows remote attackers to execute arbitrary code via unspecified vectors related to "HTTP Login," aka SAP Security Note 2197397.	10/11/2015	7.5	CVE-2015-7993
sap -- hana	The SQL interface in SAP HANA DB 1.00.73.00.389160 (NewDB100_REL) allows remote attackers to execute arbitrary code via unspecified vectors related to "SQL Login," aka SAP Security Note 2197428.	10/11/2015	7.5	CVE-2015-7994
google -- picasa	Integer overflow in Google Picasa 3.9.140 Build 239 and Build 248 allows remote attackers to execute arbitrary code via unspecified vectors related to "phase one 0x412 tag," which triggers a heap-based buffer overflow.	09/11/2015	10.0	CVE-2015-8096
oracle -- openjdk	A .desktop file in the Debian openjdk-7 package 7u79-2.5.5-1~deb8u1 includes a MIME type registration that is added to /etc/mailcap by mime-support, which allows remote attackers to execute arbitrary code via a JAR file.	09/11/2015	10.0	CVE-2014-8873
wordpress -- wordpress	SQL injection vulnerability in the wp_untrash_post_comments function in wp-includes/post.php in WordPress before 4.2.4 allows remote attackers to execute arbitrary SQL commands via a comment that is mishandled after retrieval from the trash.	09/11/2015	7.5	CVE-2015-2213
ibm -- security_access_manager_for_web	IBM Security Access Manager for Web 7.x before 7.0.0.16 and 8.x before 8.0.1.3 mishandles WebSEAL HTTPTransformation requests, which allows remote attackers to read or write to arbitrary files via unspecified vectors.	08/11/2015	7.5	CVE-2015-4963
ibm -- powerha_system_mirror	CSPOC in IBM PowerHA SystemMirror on AIX 6.1 and 7.1 allows remote authenticated users to perform an "su root" action by leveraging presence on the cluster-wide password-change list.	08/11/2015	8.5	CVE-2015-5005
ibm -- security_guardium	diag in IBM Security Guardium 8.2 before p6015, 9.0 before p6015, 9.1, 9.5, and 10.0 before p6015 allows local users to obtain root access via unspecified key sequences.	08/11/2015	7.2	CVE-2015-5043
mit -- kerberos	lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted SPNEGO packet that is mishandled during a gss_inquire_context call.	08/11/2015	7.1	CVE-2015-2695
mit -- kerberos	lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a gss_inquire_context call.	08/11/2015	7.1	CVE-2015-2696
advantech -- eki-122x_series_firmware	Advantech EKI-122x-BE devices with firmware before 1.65, EKI-132x devices with firmware before 1.98, and EKI-136x devices with firmware before 1.27 have hardcoded SSH keys, which makes it easier for remote attackers to obtain access via an SSH session.	06/11/2015	10.0	CVE-2015-6476
f5 -- big-ip_access_policy_manager	The datastor kernel module in F5 BIG-IP Analytics, APM, ASM, Link Controller, and LTM 11.1.0 before 12.0.0, BIG-IP AAM 11.4.0 before 12.0.0, BIG-IP AFM, PEM 11.3.0 before 12.0.0, BIG-IP Edge Gateway, WebAccelerator, and WOM 11.1.0 through 11.3.0, BIG-IP GTM 11.1.0 through 11.6.0, BIG-IP PSM 11.1.0 through 11.4.1, BIG-IQ Cloud and Security 4.0.0 through 4.5.0, BIG-IQ Device 4.2.0 through 4.5.0, BIG-IQ ADC 4.5.0, and Enterprise Manager 3.0.0 through 3.1.1 allows remote authenticated users to cause a denial of service or gain privileges by leveraging permission to upload and execute code.	06/11/2015	9.0	CVE-2015-7394
login_disable_project -- login_disable	The Login Disable module 6.x-1.x before 6.x-1.1 and 7.x-1.x before 7.x-1.2 for Drupal does not properly load the user_logout function, which allows remote attackers to bypass the logout protection mechanism by leveraging a contributed user authentication module, as demonstrated by the CAS and URL Login modules.	06/11/2015	7.5	CVE-2015-8082
qemu -- qemu	Buffer overflow in the vnc_refresh_server_surface function in the VNC display driver in QEMU before 2.4.0.1 allows guest users to cause a denial of service (heap memory corruption and process crash) or possibly execute arbitrary code on the host via unspecified vectors, related to refreshing the server display surface.	06/11/2015	7.2	CVE-2015-5225
qemu -- qemu	hw/ide/core.c in QEMU does not properly restrict the commands accepted by an ATAPI device, which allows guest users to cause a denial of service or possibly have unspecified other impact via certain IDE commands, as demonstrated by a WIN_READ_NATIVE_MAX command to an empty drive, which triggers a divide-by-zero error and instance crash.	06/11/2015	10.0	CVE-2015-6855

Semana 02/11/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- web_security_appliance	The proxy-cache implementation in Cisco AsyncOS 8.0.x before 8.0.7-151, 8.1.x and 8.5.x before 8.5.2-004, 8.6.x and 8.7.x before 8.7.0-171-LD, and 8.8.x before 8.8.0-085 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via multiple proxy connections, aka Bug ID CSCus10922.	06/11/2015	7.8	CVE-2015-6292
cisco -- web_security_appliance	The admin web interface in Cisco AsyncOS 8.x before 8.0.8-113, 8.1.x and 8.5.x before 8.5.3-051, 8.6.x and 8.7.x before 8.7.0-171-LD, and 8.8.x before 8.8.0-085 on Web Security Appliance (WSA) devices allows remote authenticated users to obtain root privileges via crafted certificate-generation arguments, aka Bug ID CSCus83445.	06/11/2015	9.0	CVE-2015-6298
typemoon -- fate/hollow_ataraxia	TYPE-MOON Fate/stay night, Fate/hollow ataraxia, Witch on the Holy Night, and Fate/stay night + hollow ataraxia set allow remote attackers to execute arbitrary OS commands via crafted saved data.	06/11/2015	10.0	CVE-2015-5672
cisco -- email_security_appliance	Cisco AsyncOS before 8.5.7-043, 9.x before 9.1.1-023, and 9.5.x and 9.6.x before 9.6.0-046 on Email Security Appliance (ESA) devices mishandles malformed fields during body-contains, attachment-contains, every-attachment-contains, attachment-binary-contains, dictionary-match, and attachment-dictionary-match filtering, which allows remote attackers to cause a denial of service (memory consumption) via a crafted attachment in an e-mail message, aka Bug ID CSCuv47151.	05/11/2015	7.8	CVE-2015-6291
cisco -- web_security_appliance	Cisco AsyncOS 8.x before 8.0.8-113, 8.1.x and 8.5.x before 8.5.3-051, 8.6.x and 8.7.x before 8.7.0-171-LD, and 8.8.x before 8.8.0-085 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via multiple file-range requests, aka Bug ID CSCur39155.	05/11/2015	7.8	CVE-2015-6293
cisco -- content_security_management_appliance	Cisco AsyncOS before 8.5.7-042, 9.x before 9.1.0-032, 9.1.x before 9.1.1-023, and 9.5.x and 9.6.x before 9.6.0-042 on Email Security Appliance (ESA) devices; before 9.1.0-032, 9.1.1 before 9.1.1-005, and 9.5.x before 9.5.0-025 on Content Security Management Appliance (SMA) devices; and before 7.7.0-725 and 8.x before 8.0.8-113 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (memory consumption) via a flood of TCP packets, aka Bug IDs CSCus79774, CSCus79777, and CSCzv95795.	05/11/2015	7.8	CVE-2015-6321
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	05/11/2015	7.5	CVE-2015-4513
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 42.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	05/11/2015	7.5	CVE-2015-4514
mozilla -- firefox	The sec_asn1d_parse_leaf function in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, improperly restricts access to an unspecified data structure, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data, related to a "use-after-poison" issue.	05/11/2015	7.5	CVE-2015-7181
mozilla -- firefox	Heap-based buffer overflow in the ASN.1 decoder in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data.	05/11/2015	7.5	CVE-2015-7182
mozilla -- firefox	Integer overflow in the PL_ARENA_ALLOCATE implementation in Netscape Portable Runtime (NSPR) in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.	05/11/2015	7.5	CVE-2015-7183
mozilla -- firefox	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allow remote attackers to bypass the Same Origin Policy for an IP address origin, and conduct cross-site scripting (XSS) attacks, by appending whitespace characters to an IP address string.	05/11/2015	7.5	CVE-2015-7188
mozilla -- firefox	The accessibility-tools feature in Mozilla Firefox before 42.0 on OS X improperly interacts with the implementation of the TABLE element, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by using an NSAccessibilityIndexAttribute value to reference a row index.	05/11/2015	7.5	CVE-2015-7192
mozilla -- firefox	Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 improperly follow the CORS cross-origin request algorithm for the POST method in situations involving an unspecified Content-Type header manipulation, which allows remote attackers to bypass the Same Origin Policy by leveraging the lack of a preflight-request step.	05/11/2015	7.5	CVE-2015-7193
mozilla -- firefox	Buffer underflow in libjar in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted ZIP archive.	05/11/2015	7.5	CVE-2015-7194
mozilla -- firefox	Buffer overflow in the rx::TextureStorage11 class in ANGLE, as used in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted texture data.	05/11/2015	7.5	CVE-2015-7198
mozilla -- firefox	The (1) AddWeightedPathSegLists and (2) SVGPathSegListSMILType::Interpolate functions in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 lack status checking, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted SVG document.	05/11/2015	7.5	CVE-2015-7199
mozilla -- firefox	The CryptoKey interface implementation in Mozilla Firefox before 42.0 and Firefox ESR 38.x before 38.4 lacks status checking, which allows attackers to have an unspecified impact via vectors related to a cryptographic key.	05/11/2015	7.5	CVE-2015-7200
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.16 and 11.x before 11.0.13, Acrobat and Acrobat Reader DC Classic before 2015.006.30094, and Acrobat and Acrobat Reader DC Continuous before 2015.009.20069 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via a crafted CMAP table in a PDF document, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622.	03/11/2015	9.3	CVE-2015-7650
commvault -- edge_server	The Web Console in Commvault Edge Server 10 R2 allows remote attackers to execute arbitrary OS commands via crafted serialized data in a cookie.	03/11/2015	10.0	CVE-2015-7253
google -- android	mediaserver in Android 5.x before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 19779574, 23680780, 23876444, and 23658148, a different vulnerability than CVE-2015-8072 and CVE-2015-8073.	03/11/2015	10.0	CVE-2015-6608
google -- android	libutils in Android before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted audio file, aka internal bug 22953624.	03/11/2015	10.0	CVE-2015-6609
google -- android	libstagefright in Android before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows attackers to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka internal bug 23707088.	03/11/2015	9.3	CVE-2015-6610
google -- android	libmedia in Android before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows attackers to gain privileges via a crafted application, aka internal bug 23540426.	03/11/2015	9.3	CVE-2015-6612
google -- android	mediaserver in Android 4.4 through 5.x before 5.1.1 LMY48X and 6.0 before 2015-11-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23881715, a different vulnerability than CVE-2015-6608 and CVE-2015-8073.	03/11/2015	10.0	CVE-2015-8072
google -- android	mediaserver in Android 4.4 and 5.1 before 5.1.1 LMY48X allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 14388161, a different vulnerability than CVE-2015-6608 and CVE-2015-8072.	03/11/2015	10.0	CVE-2015-8073
hp -- arcsight_command_center	HP ArcSight Logger 6.0.0.7307.1, ArcSight Command Center 6.8.0.1896.0, and ArcSight Connector Appliance 6.4.0.6881.3 use the root account to execute files owned by the arcsight user, which might allow local users to gain privileges by leveraging arcsight account access.	03/11/2015	7.2	CVE-2015-6030
hp -- vertica	The vertica-udx-zygote process in HP Vertica 7.1.1 UDx does not require authentication, which allows remote attackers to execute arbitrary commands via a crafted packet, aka ZDI-CAN-2914.	03/11/2015	7.5	CVE-2015-6867
ibm -- tivoli_storage_manager	The Reporting and Monitoring component in Tivoli Monitoring in IBM Tivoli Storage Manager 6.3 before 6.3.6 and 7.1 before 7.1.3 on Linux and AIX uses world-writable permissions for unspecified files, which allows local users to gain privileges by writing to a file.	03/11/2015	7.2	CVE-2015-4927
mobatek -- mobaxterm	The default configuration of the server in MobaXterm before 8.3 has a disabled Access Control setting and consequently does not require authentication for X11 connections, which allows remote attackers to execute arbitrary commands or obtain sensitive information via X11 packets.	03/11/2015	7.5	CVE-2015-7244
powerdns -- authoritative	The label decompression functionality in PowerDNS Recursor before 3.6.4 and 3.7.x before 3.7.3 and Authoritative (Auth) Server before 3.3.3 and 3.4.x before 3.4.5 allows remote attackers to cause a denial of service (CPU consumption or crash) via a request with a long name that refers to itself. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1868.	02/11/2015	7.8	CVE-2015-5470
wp-championship_project -- wp-championship	Multiple SQL injection vulnerabilities in cs_admin_users.php in the wp-championship plugin 5.8 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) user, (2) isadmin, (3) mail service, (4) mailresceipt, (5) stellv, (6) champtipp, (7) tippgroup, or (8) userid parameter.	02/11/2015	7.5	CVE-2015-5308
qolsys -- iq_panel	Qolsys IQ Panel (aka QOL) before 1.5.1 has hardcoded cryptographic keys, which allows remote attackers to create digital signatures for code by leveraging knowledge of a key from a different installation.	31/10/2015	9.3	CVE-2015-6032
qolsys -- iq_panel	Qolsys IQ Panel (aka QOL) before 1.5.1 does not verify the digital signatures of software updates, which allows man-in-the-middle attackers to bypass intended access restrictions via a modified update.	31/10/2015	9.3	CVE-2015-6033
xen -- xen	The mod_l2_entry function in arch/x86/mm.c in Xen 3.4 through 4.6.x does not properly validate level 2 page table entries, which allows local PV guest administrators to gain privileges via a crafted superpage mapping.	30/10/2015	7.2	CVE-2015-7835