Histórico de vulnerabilidades de Septiembre del 2015

Semana 28/09/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apport_project -- apport	kernel_crashdump in Apport before 2.19 allows local users to cause a denial of service (disk consumption) or possibly gain privileges via a (1) symlink or (2) hard link attack on /var/crash/vmcore.log.	01/10/2015	7.2	CVE-2015-1338
datalex -- airline_booking_software	Datalex airline booking software before 2015-09-03 allows remote attackers to read or write to arbitrary user data via a modified profileId parameter to (1) ValidateFormAction.do or (2) ProfileConfirmEditAddressAction.do.	01/10/2015	7.5	CVE-2015-2858
emc -- rsa_certificate_manager	Directory traversal vulnerability in EMC RSA OneStep 6.9 before build 559, as used in RSA Certificate Manager and RSA Registration Manager through 6.9 build 558 and other products, allows remote attackers to read arbitrary files via a crafted KCSOSC_ERROR_PAGE parameter.	01/10/2015	7.8	CVE-2015-4546
google -- android	libstagefright in Android through 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted metadata in a (1) MP3 or (2) MP4 file.	01/10/2015	9.3	CVE-2015-3876
google -- android	libutils in Android through 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted metadata in a (1) MP3 or (2) MP4 file, as demonstrated by an attack against use of libutils by libstagefright in Android 5.x.	01/10/2015	9.3	CVE-2015-6602
linuxcontainers -- lxc	lxc-start in lxc before 1.0.8 and 1.1.x before 1.1.4 allows local container administrators to escape AppArmor confinement via a symlink attack on a (1) mount target or (2) bind mount source.	01/10/2015	7.2	CVE-2015-1335
google -- android	Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15328708.	30/09/2015	10.0	CVE-2014-7915
google -- android	Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15342751.	30/09/2015	10.0	CVE-2014-7916
google -- android	Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15342615.	30/09/2015	10.0	CVE-2014-7917
google -- android	Integer overflow in the native_handle_create function in libcutils/native_handle.c in Android before 5.1.1 LMY48M allows attackers to obtain a different application's privileges or cause a denial of service (Binder heap memory corruption) via a crafted application, aka internal bug 19334482.	30/09/2015	9.3	CVE-2015-1528
google -- android	Integer overflow in the Bitmap_createFromParcel function in core/jni/android/graphics/Bitmap.cpp in Android before 5.1.1 LMY48I allows attackers to cause a denial of service (system_server crash) or obtain sensitive system_server memory-content information via a crafted application that leverages improper unmarshalling of bitmaps, aka internal bug 19666945.	30/09/2015	8.5	CVE-2015-1536
google -- android	Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.	30/09/2015	10.0	CVE-2015-1538
google -- android	Multiple integer underflows in the ESDS::parseESDescriptor function in ESDS.cpp in libstagefright in Android before 5.1.1 LMY48I allow remote attackers to execute arbitrary code via crafted ESDS atoms, aka internal bug 20139950, a related issue to CVE-2015-4493.	30/09/2015	10.0	CVE-2015-1539
google -- android	The MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not properly restrict size addition, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via a crafted MPEG-4 tx3g atom, aka internal bug 20923261.	30/09/2015	10.0	CVE-2015-3824
google -- android	The MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not validate the relationship between chunk sizes and skip sizes, which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted MPEG-4 covr atoms, aka internal bug 20923261.	30/09/2015	9.3	CVE-2015-3827
google -- android	The MPEG4Extractor::parse3GPPMetaData function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not enforce a minimum size for UTF-16 strings containing a Byte Order Mark (BOM), which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted 3GPP metadata, aka internal bug 20923261, a related issue to CVE-2015-3826.	30/09/2015	10.0	CVE-2015-3828
google -- android	Off-by-one error in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via crafted MPEG-4 covr atoms with a size equal to SIZE_MAX, aka internal bug 20923261.	30/09/2015	10.0	CVE-2015-3829
google -- android	Buffer overflow in the readAt function in BpMediaHTTPConnection in media/libmedia/IMediaHTTPConnection.cpp in the mediaserver service in Android before 5.1.1 LMY48I allows attackers to execute arbitrary code via a crafted application, aka internal bug 19400722.	30/09/2015	9.3	CVE-2015-3831
google -- android	Multiple buffer overflows in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I allow remote attackers to execute arbitrary code via invalid size values of NAL units in MP4 data, aka internal bug 19641538.	30/09/2015	10.0	CVE-2015-3832
google -- android	Multiple integer overflows in the BnHDCP::onTransact function in media/libmedia/IHDCP.cpp in libstagefright in Android before 5.1.1 LMY48I allow attackers to execute arbitrary code via a crafted application that uses HDCP encryption, leading to a heap-based buffer overflow, aka internal bug 20222489.	30/09/2015	10.0	CVE-2015-3834
google -- android	Buffer overflow in the OMXNodeInstance::emptyBuffer function in omx/OMXNodeInstance.cpp in libstagefright in Android before 5.1.1 LMY48I allows attackers to execute arbitrary code via a crafted application, aka internal bug 20634516.	30/09/2015	9.3	CVE-2015-3835
google -- android	The Parse_wave function in arm-wt-22k/lib_src/eas_mdls.c in the Sonivox DLS-to-EAS converter in Android before 5.1.1 LMY48I does not reject a negative value for a certain size field, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via crafted XMF data, aka internal bug 21132860.	30/09/2015	10.0	CVE-2015-3836
google -- android	The OpenSSLX509Certificate class in org/conscrypt/OpenSSLX509Certificate.java in Android before 5.1.1 LMY48I improperly includes certain context data during serialization and deserialization, which allows attackers to execute arbitrary code via an application that sends a crafted Intent, aka internal bug 21437603.	30/09/2015	9.3	CVE-2015-3837
google -- android	Multiple heap-based buffer overflows in libeffects in the Audio Policy Service in mediaserver in Android before 5.1.1 LMY48I allow attackers to execute arbitrary code via a crafted application, aka internal bug 21953516.	30/09/2015	9.3	CVE-2015-3842
google -- android	The SIM Toolkit (STK) framework in Android before 5.1.1 LMY48I allows attackers to (1) intercept or (2) emulate unspecified Telephony STK SIM commands via an application that sends a crafted Intent, related to com/android/internal/telephony/cat/AppInterface.java, aka internal bug 21697171.	30/09/2015	9.3	CVE-2015-3843
google -- android	The Region_createFromParcel function in core/jni/android/graphics/Region.cpp in Region in Android before 5.1.1 LMY48M does not check the return values of certain read operations, which allows attackers to execute arbitrary code via an application that sends a crafted message to a service, aka internal bug 21585255.	30/09/2015	9.3	CVE-2015-3849
google -- android	The checkDestination function in internal/telephony/SMSDispatcher.java in Android before 5.1.1 LMY48M relies on an obsolete permission name for an authorization check, which allows attackers to bypass an intended user-confirmation requirement for SMS short-code messaging via a crafted application, aka internal bug 22314646.	30/09/2015	9.3	CVE-2015-3858
google -- android	packages/Keyguard/res/layout/keyguard_password_view.xml in Lockscreen in Android 5.x before 5.1.1 LMY48M does not restrict the number of characters in the passwordEntry input field, which allows physically proximate attackers to bypass intended access restrictions via a long password that triggers a SystemUI crash, aka internal bug 22214934.	30/09/2015	7.2	CVE-2015-3860
google -- android	Multiple integer overflows in the Blob class in keystore/keystore.cpp in Keystore in Android before 5.1.1 LMY48M allow attackers to execute arbitrary code and read arbitrary Keystore keys via an application that uses a crafted blob in an insert operation, aka internal bug 22802399.	30/09/2015	9.3	CVE-2015-3863
google -- android	Integer underflow in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in mediaserver in Android before 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted MPEG-4 data, aka internal bug 23034759. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-3824.	30/09/2015	10.0	CVE-2015-3864
google -- android	SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I does not properly consider integer promotion, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via crafted atoms in MP4 data, aka internal bug 20139950, a different vulnerability than CVE-2015-1538. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-7915, CVE-2014-7916, and/or CVE-2014-7917.	30/09/2015	10.0	CVE-2015-6575
bisonware -- bisonftp	Directory traversal vulnerability in BisonWare BisonFTP 3.5 allows remote attackers to read arbitrary files via a ../ (dot dot slash) in a RETR command.	29/09/2015	7.8	CVE-2015-7602
codepeople -- appointment_booking_calendar	SQL injection vulnerability in cpabc_appointments_admin_int_calendar_list.inc.php in the Appointment Booking Calendar plugin before 1.1.8 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors related to updating the username.	29/09/2015	7.5	CVE-2015-7319
konicaminolta -- ftp_utility	Directory traversal vulnerability in Konica Minolta FTP Utility 1.0 allows remote attackers to read arbitrary files via a ..\ (dot dot backslash) in a RETR command.	29/09/2015	7.8	CVE-2015-7603
pcman's_ftp_server_project -- pcman's_ftp_server	Directory traversal vulnerability in PCMan's FTP Server 2.0.7 allows remote attackers to read arbitrary files via a ..// (dot dot double slash) in a RETR command.	29/09/2015	7.8	CVE-2015-7601
x2engine -- x2crm	Incomplete blacklist vulnerability in the FileUploadsFilter class in protected/components/filters/FileUploadsFilter.php in X2Engine X2CRM before 5.0.9 allows remote authenticated users to execute arbitrary PHP code by uploading a file with a .pht extension.	29/09/2015	7.5	CVE-2015-5074
endian_firewall -- endian_firewall	Endian Firewall before 3.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) NEW_PASSWORD_1 or (2) NEW_PASSWORD_2 parameter to cgi-bin/chpasswd.cgi.	28/09/2015	10.0	CVE-2015-5082
h5ai_project -- h5ai	Unrestricted file upload vulnerability in h5ai before 0.25.0 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the directory specified by the href parameter.	28/09/2015	7.5	CVE-2015-3203
qemu -- qemu	Heap-based buffer overflow in the ne2000_receive function in hw/net/ne2000.c in QEMU before 2.4.0.1 allows guest OS users to cause a denial of service (instance crash) or possibly execute arbitrary code via vectors related to receiving packets.	28/09/2015	7.2	CVE-2015-5279
roaring_penguin -- remind	Buffer overflow in the DumpSysVar function in var.c in Remind before 3.1.15 allows attackers to have unspecified impact via a long name.	28/09/2015	10.0	CVE-2015-5957
zohocorp -- manageengine_eventlog_analyzer	ZOHO ManageEngine EventLog Analyzer 10.6 build 10060 and earlier allows remote attackers to bypass intended restrictions and execute arbitrary SQL commands via an allowed query followed by a disallowed one in the query parameter to event/runQuery.do, as demonstrated by "SELECT 1;INSERT INTO."	28/09/2015	7.5	CVE-2015-7387

Histórico de vulnerabilidades de Septiembre del 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- ios	The IPv6 snooping functionality in the first-hop security subsystem in Cisco IOS 12.2, 15.0, 15.1, 15.2, 15.3, 15.4, and 15.5 and IOS XE 3.2SE, 3.3SE, 3.3XO, 3.4SG, 3.5E, and 3.6E before 3.6.3E; 3.7E before 3.7.2E; 3.9S and 3.10S before 3.10.6S; 3.11S before 3.11.4S; 3.12S and 3.13S before 3.13.3S; and 3.14S before 3.14.2S does not properly implement the Control Plane Protection (aka CPPr) feature, which allows remote attackers to cause a denial of service (device reload) via a flood of ND packets, aka Bug ID CSCus19794.	27/09/2015	7.8	CVE-2015-6278
cisco -- ios	The IPv6 snooping functionality in the first-hop security subsystem in Cisco IOS 12.2, 15.0, 15.1, 15.2, 15.3, 15.4, and 15.5 and IOS XE 3.2SE, 3.3SE, 3.3XO, 3.4SG, 3.5E, and 3.6E before 3.6.3E; 3.7E before 3.7.2E; 3.9S and 3.10S before 3.10.6S; 3.11S before 3.11.4S; 3.12S and 3.13S before 3.13.3S; and 3.14S before 3.14.2S allows remote attackers to cause a denial of service (device reload) via a malformed ND packet with the Cryptographically Generated Address (CGA) option, aka Bug ID CSCuo04400.	27/09/2015	7.8	CVE-2015-6279
cisco -- ios	The SSHv2 functionality in Cisco IOS 15.2, 15.3, 15.4, and 15.5 and IOS XE 3.6E before 3.6.3E, 3.7E before 3.7.1E, 3.10S before 3.10.6S, 3.11S before 3.11.4S, 3.12S before 3.12.3S, 3.13S before 3.13.3S, and 3.14S before 3.14.1S does not properly implement RSA authentication, which allows remote attackers to obtain login access by leveraging knowledge of a username and the associated public key, aka Bug ID CSCus73013.	27/09/2015	9.3	CVE-2015-6280
easyio -- easyio-30p-sf	EasyIO EasyIO-30P-SF controllers with firmware before 0.5.21 and 2.x before 2.0.5.21, as used in Accutrol, Bar-Tech Automation, Infocon/EasyIO, Honeywell Automation India, Johnson Controls, SyxthSENSE, Transformative Wave Technologies, Tridium Asia Pacific, and Tridium Europe products, have a hardcoded password, which makes it easier for remote attackers to obtain access via unspecified vectors.	27/09/2015	9.0	CVE-2015-3974
refbase -- refbase	install.php in Web Reference Database (aka refbase) through 0.9.6 allows remote attackers to execute arbitrary commands via the adminPassword parameter, a different issue than CVE-2015-7381.	27/09/2015	7.5	CVE-2015-6008
refbase -- refbase	Multiple SQL injection vulnerabilities in Web Reference Database (aka refbase) through 0.9.6 allow remote attackers to execute arbitrary SQL commands via (1) the where parameter to rss.php or (2) the sqlQuery parameter to search.php, a different issue than CVE-2015-7382.	27/09/2015	7.5	CVE-2015-6009
refbase -- refbase	Multiple PHP remote file inclusion vulnerabilities in install.php in Web Reference Database (aka refbase) through 0.9.6 allow remote attackers to execute arbitrary PHP code via the (1) pathToMYSQL or (2) databaseStructureFile parameter, a different issue than CVE-2015-6008.	27/09/2015	7.5	CVE-2015-7381
refbase -- refbase	SQL injection vulnerability in install.php in Web Reference Database (aka refbase) through 0.9.6 allows remote attackers to execute arbitrary SQL commands via the defaultCharacterSet parameter, a different issue than CVE-2015-6009.	27/09/2015	7.5	CVE-2015-7382
cisco -- ios_xe	Cisco IOS XE 2.x and 3.x before 3.10.6S, 3.11.xS through 3.13.xS before 3.13.3S, and 3.14.xS through 3.15.xS before 3.15.1S allows remote attackers to cause a denial of service (device reload) via IPv4 packets that require NAT and MPLS actions, aka Bug ID CSCut96933.	25/09/2015	7.8	CVE-2015-6282
cisco -- anyconnect_secure_mobility_client	Untrusted search path vulnerability in the CMainThread::launchDownloader function in vpndownloader.exe in Cisco AnyConnect Secure Mobility Client 2.0 through 4.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by dbghelp.dll, aka Bug ID CSCuv01279. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4211.	25/09/2015	7.2	CVE-2015-6305
cisco -- anyconnect_secure_mobility_client	Cisco AnyConnect Secure Mobility Client 4.1(8) on OS X and Linux does not verify pathnames before installation actions, which allows local users to obtain root privileges via a crafted installation file, aka Bug ID CSCuv11947.	25/09/2015	7.2	CVE-2015-6306
indusoft -- web_studio	The Remote Agent component in Schneider Electric InduSoft Web Studio before 8.0 allows remote attackers to execute arbitrary code via unspecified vectors, aka ZDI-CAN-2649.	25/09/2015	7.5	CVE-2015-7374
indusoft -- web_studio	Schneider Electric InduSoft Web Studio before 8.0 allows remote attackers to execute arbitrary code or cause a denial of service (unhandled runtime exception and application crash) via a crafted Indusoft Project file.	25/09/2015	7.5	CVE-2015-7375

Semana 21/09/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	24/09/2015	7.5	CVE-2015-4500
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 41.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	24/09/2015	7.5	CVE-2015-4501
mozilla -- firefox	Use-after-free vulnerability in the HTMLVideoElement interface in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 allows remote attackers to execute arbitrary code via crafted JavaScript code that modifies the URI table of a media element, aka ZDI-CAN-3176.	24/09/2015	7.5	CVE-2015-4509
mozilla -- firefox	Mozilla Firefox before 41.0 allows remote attackers to bypass certain ECMAScript 5 (aka ES5) API protection mechanisms and modify immutable properties, and consequently execute arbitrary JavaScript code with chrome privileges, via a crafted web page that does not use ES5 APIs.	24/09/2015	9.3	CVE-2015-4516
mozilla -- firefox	NetworkUtils.cpp in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	24/09/2015	7.5	CVE-2015-4517
mozilla -- firefox	The ConvertDialogOptions function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	24/09/2015	7.5	CVE-2015-4521
mozilla -- firefox	The nsUnicodeToUTF8::GetMaxLength function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."	24/09/2015	7.5	CVE-2015-4522
mozilla -- firefox	The nsAttrAndChildArray::GrowBy function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."	24/09/2015	7.5	CVE-2015-7174
mozilla -- firefox	The XULContentSinkImpl::AddText function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors, related to an "overflow."	24/09/2015	7.5	CVE-2015-7175
mozilla -- firefox	The AnimationThread function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 uses an incorrect argument to the sscanf function, which might allow remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via unknown vectors.	24/09/2015	7.5	CVE-2015-7176
mozilla -- firefox	The InitTextures function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	24/09/2015	7.5	CVE-2015-7177
mozilla -- firefox	The ProgramBinary::linkAttributes function in libGLES in ANGLE, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 on Windows, mishandles shader access, which allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted (1) OpenGL or (2) WebGL content.	24/09/2015	7.5	CVE-2015-7178
mozilla -- firefox	The VertexBufferInterface::reserveVertexSpace function in libGLES in ANGLE, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 on Windows, incorrectly allocates memory for shader attribute arrays, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via crafted (1) OpenGL or (2) WebGL content.	24/09/2015	7.5	CVE-2015-7179
mozilla -- firefox	The ReadbackResultWriterD3D11::Run function in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3 misinterprets the return value of a function call, which might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	24/09/2015	7.5	CVE-2015-7180
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5579.	22/09/2015	10.0	CVE-2015-5567
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.	22/09/2015	10.0	CVE-2015-5568
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5574, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.	22/09/2015	10.0	CVE-2015-5570
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."	22/09/2015	10.0	CVE-2015-5573
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.	22/09/2015	10.0	CVE-2015-5574
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5575
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5577
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5578
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5567.	22/09/2015	10.0	CVE-2015-5579
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5580
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5584, and CVE-2015-6682.	22/09/2015	10.0	CVE-2015-5581
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5588, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5582
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-6682.	22/09/2015	10.0	CVE-2015-5584
adobe -- air	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors.	22/09/2015	10.0	CVE-2015-5587
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-6677.	22/09/2015	10.0	CVE-2015-5588
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6678.	22/09/2015	10.0	CVE-2015-6676
adobe -- air	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-5588.	22/09/2015	10.0	CVE-2015-6677

Histórico de vulnerabilidades de Septiembre del 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6676.	22/09/2015	10.0	CVE-2015-6678
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-5584.	22/09/2015	10.0	CVE-2015-6682
avira -- management_console	Use-after-free vulnerability in the Update Manager service in Avira Management Console allows remote attackers to execute arbitrary code via a large header.	21/09/2015	10.0	CVE-2015-7303
philippine_long_distance_telephone -- kasda_kw58293_firmware	Buffer overflow in form2ping.cgi on Philippine Long Distance Telephone (PLDT) SpeedSurf 504AN devices with firmware GAN9.8U26-4-TX-R6B018-PH.EN and Kasda KW58293 devices allows remote attackers to cause a denial of service (device outage) via a long ipaddr parameter.	21/09/2015	7.8	CVE-2015-5993
securifi -- almond-2015_firmware	Securifi Almond devices with firmware before AL1-R201EXP10-L304-W34 and Almond-2015 devices with firmware before AL2-R088M have a default password of admin for the admin account, which allows remote attackers to obtain web-management access by leveraging the ability to authenticate from the intranet.	21/09/2015	7.3	CVE-2015-2915
vboxcomm -- satellite_express_protocol	The ndvbs module in VBox Communications Satellite Express Protocol 2.3.17.3 allows local users to write to arbitrary physical memory locations and gain privileges via a 0x00000ffd ioctl call.	21/09/2015	7.2	CVE-2015-6923
cisco -- telepresence_server_software	Buffer overflow in the Conference Control Protocol API implementation in Cisco TelePresence Server software before 4.1(2.33) on 7010, MSE 8710, Multiparty Media 310 and 320, and Virtual Machine devices allows remote attackers to cause a denial of service (device crash) via a crafted URL, aka Bug ID CSCuu28277.	20/09/2015	7.8	CVE-2015-6284
symantec -- web_gateway	The management console on Symantec Web Gateway (SWG) appliances with software before 5.2.2 DB 5.0.0.1277 allows remote authenticated users to bypass intended access restrictions and execute arbitrary commands by leveraging a "redirect."	20/09/2015	8.5	CVE-2015-5690
symantec -- web_gateway	admin_messages.php in the management console on Symantec Web Gateway (SWG) appliances with software before 5.2.2 DB 5.0.0.1277 allows remote authenticated users to execute arbitrary code by uploading a file with a safe extension and content type, and then leveraging an improper Sudo configuration to make this a setuid-root file.	20/09/2015	7.9	CVE-2015-5692
symantec -- web_gateway	The management console on Symantec Web Gateway (SWG) appliances with software before 5.2.2 DB 5.0.0.1277 allows remote authenticated users to execute arbitrary commands via vectors related to "traffic capture."	20/09/2015	7.9	CVE-2015-5693
symantec -- web_gateway	The management console on Symantec Web Gateway (SWG) appliances with software before 5.2.2 DB 5.0.0.1277 allows remote authenticated users to execute arbitrary commands at boot time via unspecified vectors.	20/09/2015	8.3	CVE-2015-6547
cisco -- prime_collaboration_assurance	The web framework in Cisco Prime Collaboration Assurance before 10.5.1.53684-1 allows remote authenticated users to bypass intended access restrictions, and create administrative accounts or read data from arbitrary tenant domains, via a crafted URL, aka Bug IDs CSCus62671 and CSCus62652.	19/09/2015	9.0	CVE-2015-4304
cisco -- prime_collaboration_assurance	The web framework in Cisco Prime Collaboration Assurance before 10.5.1.53684-1 allows remote authenticated users to bypass intended login-session read restrictions, and impersonate administrators of arbitrary tenant domains, by discovering a session identifier and constructing a crafted URL, aka Bug IDs CSCus88343 and CSCus88334.	19/09/2015	8.5	CVE-2015-4306
cisco -- prime_collaboration_provisioning	The web framework in Cisco Prime Collaboration Provisioning before 11.0 allows remote authenticated users to bypass intended access restrictions and create administrative accounts via a crafted URL, aka Bug ID CSCut64111.	19/09/2015	9.0	CVE-2015-4307
3s-smart -- codesys_gateway_server	Multiple heap-based buffer overflows in 3S-Smart CODESYS Gateway Server before 2.3.9.47 allow remote attackers to execute arbitrary code via opcode (1) 0x3ef or (2) 0x3f0.	18/09/2015	7.5	CVE-2015-6460
apple -- mac_os_x_server	Multiple unspecified vulnerabilities in Twisted in Wiki Server in Apple OS X Server before 5.0.3 allow attackers to have an unknown impact via an XML document.	18/09/2015	10.0	CVE-2015-5911
boxoft -- boxoft_wav_to_mp3_converter	Buffer overflow in Boxoft WAV to MP3 Converter allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted WAV file.	18/09/2015	7.5	CVE-2015-7243
cisco -- prime_network_registrar	Cisco Prime Network Registrar (CPNR) 8.1(3.3), 8.2(3), and 8.3(2) has a default account, which allows local users to obtain root access by leveraging knowledge of the credentials, aka Bug ID CSCuw21825.	18/09/2015	7.2	CVE-2015-6296
ge -- mds_pulsenet	GE Digital Energy MDS PulseNET and MDS PulseNET Enterprise before 3.1.5 have hardcoded credentials for a support account, which allows remote attackers to obtain administrative access, and consequently execute arbitrary code, by leveraging knowledge of the password.	18/09/2015	9.0	CVE-2015-6456
ge -- mds_pulsenet	Absolute path traversal vulnerability in the download feature in FileDownloadServlet in GE Digital Energy MDS PulseNET and MDS PulseNET Enterprise before 3.1.5 allows remote attackers to read or delete arbitrary files via a full pathname.	18/09/2015	10.0	CVE-2015-6459
sap -- netweaver_j2ee_engine	SQL injection vulnerability in the BP_FIND_JOBS_WITH_PROGRAM function module in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	18/09/2015	7.5	CVE-2015-7239
sqlite -- sqlite	Multiple unspecified vulnerabilities in SQLite before 3.8.10.2, as used in Apple iOS before 9, have unknown impact and attack vectors.	18/09/2015	10.0	CVE-2015-5895

Semana 14/09/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- iphone_os	IOMobileFrameBuffer in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	18/09/2015	7.2	CVE-2015-5843
apple -- iphone_os	IOKit in the kernel in Apple iOS before 9 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2015-5845 and CVE-2015-5846.	18/09/2015	9.3	CVE-2015-5844
apple -- iphone_os	IOKit in the kernel in Apple iOS before 9 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2015-5844 and CVE-2015-5846.	18/09/2015	9.3	CVE-2015-5845
apple -- iphone_os	IOKit in the kernel in Apple iOS before 9 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2015-5844 and CVE-2015-5845.	18/09/2015	9.3	CVE-2015-5846
apple -- iphone_os	The Disk Images component in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	18/09/2015	7.2	CVE-2015-5847
apple -- iphone_os	IOAcceleratorFamily in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	18/09/2015	7.2	CVE-2015-5848
apple -- iphone_os	IOHIDFamily in Apple iOS before 9 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	18/09/2015	9.3	CVE-2015-5867
apple -- iphone_os	The kernel in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5896 and CVE-2015-5903.	18/09/2015	7.2	CVE-2015-5868
apple -- itunes	CoreText in Apple iOS before 9 and iTunes before 12.3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file.	18/09/2015	7.5	CVE-2015-5874
apple -- iphone_os	dyld in Dev Tools in Apple iOS before 9 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	18/09/2015	9.3	CVE-2015-5876
apple -- iphone_os	The processor_set_tasks API implementation in Apple iOS before 9 allows local users to bypass an entitlement protection mechanism and obtain access to the task ports of arbitrary processes by leveraging root privileges.	18/09/2015	7.2	CVE-2015-5882
apple -- iphone_os	The kernel in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5868 and CVE-2015-5903.	18/09/2015	7.2	CVE-2015-5896
apple -- iphone_os	libpthread in the kernel in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	18/09/2015	7.2	CVE-2015-5899
apple -- iphone_os	The kernel in Apple iOS before 9 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5868 and CVE-2015-5896.	18/09/2015	10.0	CVE-2015-5903
teiko -- farol	SQL injection vulnerability in the web application in Farol allows remote attackers to execute arbitrary SQL commands via the email parameter to tkmonitor/estrutura/login/Login.actions.php.	17/09/2015	7.5	CVE-2015-6962
checkmarx -- cxsast	Checkmarx CxSAST (formerly CxSuite) before 7.1.8 allows remote authenticated users to bypass the CxQL sandbox protection mechanism and execute arbitrary C# code by asserting the (1) System.Security.Permissions.PermissionState.Unrestricted or (2) System.Security.Permissions.SecurityPermissionFlag.AllFlags permission.	16/09/2015	9.0	CVE-2014-8778
ciphercoin -- wp_limit_login_attempts	Multiple SQL injection vulnerabilities in the getip function in wp-limit-login-attempts.php in the WP Limit Login Attempts plugin before 2.0.1 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) X-Forwarded-For or (2) Client-IP HTTP header.	16/09/2015	7.5	CVE-2015-6829
sis -- windows_vga_display_manager	Silicon Integrated Systems WindowsXP Display Manager (aka VGA Driver Manager and VGA Display Manager) 6.14.10.3930 allows local users to gain privileges via a crafted (1) 0x96002400 or (2) 0x96002404 IOCTL call.	16/09/2015	7.2	CVE-2015-5465
unit4 -- teta_web	Unit4 Polska TETA Web (formerly TETA Galactica) 22.62.3.4 does not properly restrict access to the (1) Design Mode and (2) Debug Logger mode modules, which allows remote attackers to gain privileges via crafted "received parameters."	16/09/2015	7.5	CVE-2015-1173
asus -- tm-1900	Stack-based buffer overflow in the ASUS TM-AC1900 router allows remote attackers to execute arbitrary code via crafted HTTP header values.	15/09/2015	9.3	CVE-2015-6949
borland -- accurev	Multiple stack-based buffer overflows in the Reprise License Manager service in Borland AccuRev allow remote attackers to execute arbitrary code via the (1) akey or (2) actserver parameter to the the activate_doit function or (3) licfile parameter to the service_startup_doit functionality.	15/09/2015	9.3	CVE-2015-6946
ibm -- http_server	Stack-based buffer overflow in the Administration Server in IBM HTTP Server 6.1.0.x through 6.1.0.47, 7.0.0.x before 7.0.0.39, 8.0.0.x before 8.0.0.12, and 8.5.x before 8.5.5.7, as used in WebSphere Application Server and other products, allows remote authenticated users to execute arbitrary code via unspecified vectors.	15/09/2015	9.0	CVE-2015-4947
ibs_mappro_project -- ibs_mappro	Absolute path traversal vulnerability in lib/download.php in the IBS Mappro plugin before 1.0 for WordPress allows remote attackers to read arbitrary files via a full pathname in the file parameter.	15/09/2015	7.8	CVE-2015-5472
ibm -- websphere_portal	IBM WebSphere Portal 6.1.0.x through 6.1.0.6 CF27, 6.1.5.x through 6.1.5.3 CF27, 7.0.x through 7.0.0.2 CF29, 8.0.x before 8.0.0.1 CF17, and 8.5.0 before CF06 allows remote attackers to cause a denial of service (CPU and memory consumption) via a crafted request.	14/09/2015	7.8	CVE-2015-1943
impero -- impero_education_pro	Impero Education Pro before 5105 uses a hardcoded CBC key and initialization vector derived from a hash of the Imp3ro string, which makes it easier for remote attackers to obtain plaintext data by sniffing the network for ciphertext data.	14/09/2015	7.8	CVE-2015-5997
impero -- impero_education_pro	Impero Education Pro before 5105 relies on the -1|AUTHENTICATE\x02PASSWORD string for authentication, which allows remote attackers to execute arbitrary programs via an encrypted command.	14/09/2015	10.0	CVE-2015-5998
mozilla -- bugzilla	Util.pm in Bugzilla 2.x, 3.x, and 4.x before 4.2.15, 4.3.x and 4.4.x before 4.4.10, and 5.x before 5.0.1 mishandles long e-mail addresses during account registration, which allows remote attackers to obtain the default privileges for an arbitrary domain name by placing that name in a substring of an address, as demonstrated by truncation of an @mozilla.com.example.com address to an @mozilla.com address.	13/09/2015	7.5	CVE-2015-4499
advantech -- webaccess	Multiple stack-based buffer overflows in unspecified DLL files in Advantech WebAccess before 8.0.1 allow remote attackers to execute arbitrary code via unknown vectors.	11/09/2015	10.0	CVE-2014-9208
mindbite -- sitefactory_cms	Absolute path traversal vulnerability in SiteFactory CMS 5.5.9 allows remote attackers to read arbitrary files via a full pathname in the file parameter to assets/download.aspx.	11/09/2015	7.8	CVE-2015-6914
montala -- resourcespace	SQL injection vulnerability in Montala Limited ResourceSpace 7.3.7009 and earlier allows remote attackers to execute arbitrary SQL commands via the "user" cookie to plugins/feedback/pages/feedback.php.	11/09/2015	7.5	CVE-2015-6915
moxa -- eds-405a_firmware	The administrative web interface on Moxa EDS-405A and EDS-408A switches with firmware before 3.6 allows remote authenticated users to bypass a read-only protection mechanism by using Firefox with a web-developer plugin.	11/09/2015	8.5	CVE-2015-6464
sma_solar_technology_ag -- webbox_firmware	SMA Solar Sunny WebBox has hardcoded passwords, which makes it easier for remote attackers to obtain access via unspecified vectors.	11/09/2015	10.0	CVE-2015-3964
synology -- video_station	SQL injection vulnerability in Synology Video Station before 1.5-0757 allows remote attackers to execute arbitrary SQL commands via the id parameter to audiotrack.cgi.	11/09/2015	7.5	CVE-2015-6910
synology -- video_station	SQL injection vulnerability in Synology Video Station before 1.5-0763 allows remote attackers to execute arbitrary SQL commands via the id parameter to watchstatus.cgi.	11/09/2015	7.5	CVE-2015-6911
synology -- video_station	Synology Video Station before 1.5-0763 allows remote attackers to execute arbitrary shell commands via shell metacharacters in the subtitle_codepage parameter to subtitle.cgi.	11/09/2015	10.0	CVE-2015-6912
yahoo -- messenger	Multiple stack-based buffer overflows in Yahoo! Messenger 11.5.0.228 and earlier allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the (1) shortcut or (2) title keys in an emoticons.xml file.	11/09/2015	9.3	CVE-2014-7216

Semana 07/09/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- shockwave_player	Adobe Shockwave Player before 12.2.0.162 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-6681.	08/09/2015	10.0	CVE-2015-6680
adobe -- shockwave_player	Adobe Shockwave Player before 12.2.0.162 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-6680.	08/09/2015	10.0	CVE-2015-6681
libvdpau_project -- libvdpau	libvdpau before 1.1.1, when used in a setuid or setgid application, allows local users to gain privileges via unspecified vectors, related to the VDPAU_DRIVER_PATH environment variable.	08/09/2015	7.2	CVE-2015-5198
libvdpau_project -- libvdpau	Directory traversal vulnerability in dlopen in libvdpau before 1.1.1 allows local users to gain privileges via the VDPAU_DRIVER environment variable.	08/09/2015	7.2	CVE-2015-5199
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2491 and CVE-2015-2541.	08/09/2015	9.3	CVE-2015-2485
microsoft -- edge	Microsoft Internet Explorer 7 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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2486
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2487
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2490
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2485 and CVE-2015-2541.	08/09/2015	9.3	CVE-2015-2491
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2494, CVE-2015-2498, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2492
microsoft -- internet_explorer	The (1) VBScript and (2) JScript engines in Microsoft Internet Explorer 8 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."	08/09/2015	9.3	CVE-2015-2493
microsoft -- edge	Microsoft Internet Explorer 7 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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2498, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2494
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, and CVE-2015-2499.	08/09/2015	9.3	CVE-2015-2498
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2492, CVE-2015-2494, and CVE-2015-2498.	08/09/2015	9.3	CVE-2015-2499
microsoft -- internet_explorer	Microsoft Internet Explorer 7 and 8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."	08/09/2015	9.3	CVE-2015-2500
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 "Memory Corruption Vulnerability."	08/09/2015	9.3	CVE-2015-2501
microsoft -- .net_framework	Microsoft .NET Framework 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6 improperly counts objects before performing an array copy, which allows remote attackers to (1) execute arbitrary code via a crafted XAML browser application (XBAP) or (2) bypass Code Access Security restrictions via a crafted .NET Framework application, aka ".NET Elevation of Privilege Vulnerability."	08/09/2015	9.3	CVE-2015-2504
microsoft -- windows_10	atmfd.dll in 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 allows remote attackers to cause a denial of service (system crash) via a crafted OpenType font, aka "OpenType Font Parsing Vulnerability."	08/09/2015	9.3	CVE-2015-2506
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 allows local users to gain privileges via a crafted application, aka "Font Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2512.	08/09/2015	7.2	CVE-2015-2507
microsoft -- windows_10	The Adobe Type Manager Library in Microsoft Windows 10 allows local users to gain privileges via a crafted application, aka "Font Driver Elevation of Privilege Vulnerability."	08/09/2015	7.2	CVE-2015-2508
microsoft -- windows_7	Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted Media Center link (mcl) file, aka "Windows Media Center RCE Vulnerability."	08/09/2015	9.3	CVE-2015-2509
microsoft -- live_meeting_console	Buffer overflow in the Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Lync 2010, Lync 2010 Attendee, Lync 2013 SP1, Lync Basic 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted OpenType font, aka "Graphics Component Buffer Overflow Vulnerability."	08/09/2015	9.3	CVE-2015-2510
microsoft -- windows_10	The kernel-mode driver 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 allows local users to gain privileges via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2517, CVE-2015-2518, and CVE-2015-2546.	08/09/2015	7.2	CVE-2015-2511
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 allows local users to gain privileges via a crafted application, aka "Font Driver Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2507.	08/09/2015	7.2	CVE-2015-2512
microsoft -- windows_10	Windows Journal 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 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka "Windows Journal RCE Vulnerability," a different vulnerability than CVE-2015-2514 and CVE-2015-2530.	08/09/2015	9.3	CVE-2015-2513
microsoft -- windows_10	Windows Journal 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 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka "Windows Journal RCE Vulnerability," a different vulnerability than CVE-2015-2513 and CVE-2015-2530.	08/09/2015	9.3	CVE-2015-2514
microsoft -- windows_10	The kernel-mode driver 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 allows local users to gain privileges via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2511, CVE-2015-2518, and CVE-2015-2546.	08/09/2015	7.2	CVE-2015-2517
microsoft -- windows_10	The kernel-mode driver 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 allows local users to gain privileges via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2546.	08/09/2015	7.2	CVE-2015-2518
microsoft -- windows_10	Integer overflow in Windows Journal 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 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka "Windows Journal Integer Overflow RCE Vulnerability."	08/09/2015	9.3	CVE-2015-2519
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011 and 2016, 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."	08/09/2015	9.3	CVE-2015-2520
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	08/09/2015	9.3	CVE-2015-2521
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel for Mac 2011 and 2016, 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."	08/09/2015	9.3	CVE-2015-2523
microsoft -- windows_10	Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka "Windows Task Management Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2528.	08/09/2015	7.2	CVE-2015-2524
microsoft -- windows_10	Task Scheduler 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 allows local users to bypass intended filesystem restrictions and delete arbitrary files via unspecified vectors, aka "Windows Task File Deletion Elevation of Privilege Vulnerability."	08/09/2015	7.2	CVE-2015-2525
microsoft -- windows_10	The process-initialization implementation in win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 does not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	08/09/2015	7.2	CVE-2015-2527

Histórico de vulnerabilidades de Septiembre del 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 do not properly constrain impersonation levels, which allows local users to gain privileges via a crafted application, aka "Windows Task Management Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2524.	08/09/2015	7.2	CVE-2015-2528
microsoft -- windows_10	Windows Journal 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 allows remote attackers to execute arbitrary code via a crafted .jnt file, aka "Windows Journal RCE Vulnerability," a different vulnerability than CVE-2015-2513 and CVE-2015-2514.	08/09/2015	9.3	CVE-2015-2530
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 "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2485 and CVE-2015-2491.	08/09/2015	9.3	CVE-2015-2541
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 "Memory Corruption Vulnerability."	08/09/2015	9.3	CVE-2015-2542
microsoft -- office	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2013 RT SP1 allows remote attackers to execute arbitrary code via a crafted EPS image, aka "Microsoft Office Malformed EPS File Vulnerability."	08/09/2015	9.3	CVE-2015-2545
microsoft -- windows_10	The kernel-mode driver 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 allows local users to gain privileges via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-2511, CVE-2015-2517, and CVE-2015-2518.	08/09/2015	7.2	CVE-2015-2546
ffmpeg -- ffmpeg	The decode_ihdr_chunk function in libavcodec/pngdec.c in FFmpeg before 2.7.2 does not enforce uniqueness of the IHDR (aka image header) chunk in a PNG image, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted image with two or more of these chunks.	05/09/2015	7.5	CVE-2015-6818
ffmpeg -- ffmpeg	Multiple integer underflows in the ff_mjpeg_decode_frame function in libavcodec/mjpegdec.c in FFmpeg before 2.7.2 allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted MJPEG data.	05/09/2015	7.5	CVE-2015-6819
ffmpeg -- ffmpeg	The ff_sbr_apply function in libavcodec/aacsbr.c in FFmpeg before 2.7.2 does not check for a matching AAC frame syntax element before proceeding with Spectral Band Replication calculations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted AAC data.	05/09/2015	7.5	CVE-2015-6820
ffmpeg -- ffmpeg	The ff_mpv_common_init function in libavcodec/mpegvideo.c in FFmpeg before 2.7.2 does not properly maintain the encoding context, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via crafted MPEG data.	05/09/2015	7.5	CVE-2015-6821
ffmpeg -- ffmpeg	The destroy_buffers function in libavcodec/sanm.c in FFmpeg before 2.7.2 does not properly maintain height and width values in the video context, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via crafted LucasArts Smush video data.	05/09/2015	7.5	CVE-2015-6822
ffmpeg -- ffmpeg	The allocate_buffers function in libavcodec/alac.c in FFmpeg before 2.7.2 does not initialize certain context data, which allows remote attackers to cause a denial of service (segmentation violation) or possibly have unspecified other impact via crafted Apple Lossless Audio Codec (ALAC) data.	05/09/2015	7.5	CVE-2015-6823
ffmpeg -- ffmpeg	The sws_init_context function in libswscale/utils.c in FFmpeg before 2.7.2 does not initialize certain pixbuf data structures, which allows remote attackers to cause a denial of service (segmentation violation) or possibly have unspecified other impact via crafted video data.	05/09/2015	7.5	CVE-2015-6824
ffmpeg -- ffmpeg	The ff_frame_thread_init function in libavcodec/pthread_frame.c in FFmpeg before 2.7.2 mishandles certain memory-allocation failures, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via a crafted file, as demonstrated by an AVI file.	05/09/2015	7.5	CVE-2015-6825
ffmpeg -- ffmpeg	The ff_rv34_decode_init_thread_copy function in libavcodec/rv34.c in FFmpeg before 2.7.2 does not initialize certain structure members, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via crafted (1) RV30 or (2) RV40 RealVideo data.	05/09/2015	7.5	CVE-2015-6826
isc -- bind	buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.	04/09/2015	7.8	CVE-2015-5722
isc -- bind	openpgpkey_61.c in named in ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted DNS response.	04/09/2015	7.1	CVE-2015-5986