Semana 26/10/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fedoraproject -- 389_directory_server	389 Directory Server (formerly Fedora Directory Server) before 1.3.3.12 does not enforce the nsSSL3Ciphers preference when creating an sslSocket, which allows remote attackers to have unspecified impact by requesting to use a disabled cipher.	29/10/2015	7.5	CVE-2015-3230
ibm -- domino	Buffer overflow in IBM Domino 8.5.1 through 8.5.3 before 8.5.3 FP6 IF10 and 9.x before 9.0.1 FP4 IF3 allows remote attackers to execute arbitrary code or cause a denial of service (SMTP daemon crash) via a crafted GIF image, aka SPRs KLYH9ZDKRE and KLYH9ZTLEZ, a different vulnerability than CVE-2015-5040.	29/10/2015	7.5	CVE-2015-4994
ibm -- domino	Buffer overflow in IBM Domino 8.5.1 through 8.5.3 before 8.5.3 FP6 IF10 and 9.x before 9.0.1 FP4 IF3 allows remote attackers to execute arbitrary code or cause a denial of service (SMTP daemon crash) via a crafted GIF image, aka SPRs KLYH9ZDKRE and KLYH9ZTLEZ, a different vulnerability than CVE-2015-4994.	29/10/2015	7.5	CVE-2015-5040
joomla -- joomla!	SQL injection vulnerability in Joomla! 3.2 before 3.4.4 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, a different vulnerability than CVE-2015-7858.	29/10/2015	7.5	CVE-2015-7297
joomla -- joomla!	SQL injection vulnerability in the getListQuery function in administrator/components/com_contenthistory/models/history.php in Joomla! 3.2 before 3.4.5 allows remote attackers to execute arbitrary SQL commands via the list[select] parameter to index.php.	29/10/2015	7.5	CVE-2015-7857
joomla -- joomla!	SQL injection vulnerability in Joomla! 3.2 before 3.4.4 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, a different vulnerability than CVE-2015-7297.	29/10/2015	7.5	CVE-2015-7858
medicomp -- medcin_engine	The AddUserFinding implementation in Medicomp MEDCIN Engine 2.22.20153.x before 2.22.20153.226 might allow remote attackers to execute arbitrary code or cause a denial of service (integer truncation and heap-based buffer overflow) via a crafted packet on port 8190.	29/10/2015	7.5	CVE-2015-6006
techno_project_japan -- enisys_gw	SQL injection vulnerability in Techno Project Japan Enisys Gw before 1.4.1 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	29/10/2015	7.5	CVE-2015-5668
adobe -- shockwave_player	Adobe Shockwave Player before 12.2.1.171 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	28/10/2015	10.0	CVE-2015-7649
janitza -- umg_508	The FTP service on Janitza UMG 508, 509, 511, 604, and 605 devices has a default password, which makes it easier for remote attackers to read or write to files via a session on TCP port 21.	28/10/2015	7.5	CVE-2015-3968
janitza -- umg_508	The debug interface on Janitza UMG 508, 509, 511, 604, and 605 devices does not require authentication, which allows remote attackers to read or write to files, or execute arbitrary JASIC code, via a session on TCP port 1239.	28/10/2015	7.5	CVE-2015-3971
janitza -- umg_508	The web interface on Janitza UMG 508, 509, 511, 604, and 605 devices supports only short PIN values for authentication, which makes it easier for remote attackers to obtain access via a brute-force attack.	28/10/2015	10.0	CVE-2015-3972
rockwellautomation -- micrologix_1100_firmware	Stack-based buffer overflow on Allen-Bradley MicroLogix 1100 devices before B FRN 15.000 and 1400 devices through B FRN 15.003 allows remote attackers to execute arbitrary code via unspecified vectors.	28/10/2015	10.0	CVE-2015-6490
rockwellautomation -- micrologix_1100_firmware	Allen-Bradley MicroLogix 1100 devices before B FRN 15.000 and 1400 devices before B FRN 15.003 allow remote attackers to cause a denial of service (memory corruption and device crash) via a crafted HTTP request.	28/10/2015	7.8	CVE-2015-6492
sap -- hana	The index server (hdbindexserver) in SAP HANA 1.00.095 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via an HTTP request, aka SAP Security Note 2197428.	27/10/2015	7.5	CVE-2015-7986
owncloud -- owncloud	Directory traversal vulnerability in ownCloud Server before 8.0.6 and 8.1.x before 8.1.1 allows remote authenticated users to list directory contents and possibly cause a denial of service (CPU consumption) via a .. (dot dot) in the dir parameter to index.php/apps/files/ajax/scan.php.	26/10/2015	7.5	CVE-2015-6500
owncloud -- owncloud	The files_external app in ownCloud Server before 7.0.9, 8.0.x before 8.0.7, and 8.1.x before 8.1.2 allows remote authenticated users to instantiate arbitrary classes and possibly execute arbitrary code via a crafted mount point option, related to "objectstore."	26/10/2015	9.0	CVE-2015-7699
ibm -- general_parallel_file_system	IBM General Parallel File System (GPFS) 3.5.x before 3.5.0.27 and 4.1.x before 4.1.1.2 and Spectrum Scale 4.1.1.x before 4.1.1.2 allow local users to obtain root privileges for command execution via unspecified vectors.	25/10/2015	7.2	CVE-2015-4974
ibm -- cognos_disclosure_management	IBM Cognos Disclosure Management (CDM) 10.1.x and 10.2.x before 10.2.4 IF10 allows man-in-the-middle attackers to obtain access by spoofing an executable file during a client upload operation.	25/10/2015	9.3	CVE-2015-5014
cisco -- adaptive_security_appliance_software	The DHCPv6 relay implementation in Cisco Adaptive Security Appliance (ASA) software 9.0 before 9.0(4.37), 9.1 before 9.1(6.6), 9.2 before 9.2(4), 9.3 before 9.3(3.5), and 9.4 before 9.4(2) allows remote attackers to cause a denial of service (device reload) via crafted DHCPv6 packets, aka Bug IDs CSCus56252 and CSCus57142.	24/10/2015	7.1	CVE-2015-6324
cisco -- adaptive_security_appliance_software	Cisco Adaptive Security Appliance (ASA) software 7.2 and 8.2 before 8.2(5.58), 8.3 and 8.4 before 8.4(7.29), 8.5 through 8.7 before 8.7(1.17), 9.0 before 9.0(4.37), 9.1 before 9.1(6.4), 9.2 before 9.2(4), 9.3 before 9.3(3.1), and 9.4 before 9.4(1.1) allows remote attackers to cause a denial of service (device reload) via a crafted DNS response, aka Bug ID CSCut03495.	24/10/2015	7.1	CVE-2015-6325
cisco -- adaptive_security_appliance_software	Cisco Adaptive Security Appliance (ASA) software 7.2 and 8.2 before 8.2(5.58), 8.3 and 8.4 before 8.4(7.29), 8.5 through 8.7 before 8.7(1.17), 9.0 before 9.0(4.37), 9.1 before 9.1(6.6), 9.2 before 9.2(4), 9.3 before 9.3(3.5), and 9.4 before 9.4(1.5) allows remote attackers to cause a denial of service (device reload) via a crafted DNS response, aka Bug ID CSCuu07799.	24/10/2015	7.8	CVE-2015-6326
cisco -- adaptive_security_appliance_software	The IKEv1 implementation in Cisco Adaptive Security Appliance (ASA) software 7.2 and 8.2 before 8.2(5.58), 8.3 and 8.4 before 8.4(7.29), 8.5 through 8.7 before 8.7(1.17), 9.0 before 9.0(4.37), 9.1 before 9.1(6.8), 9.2 before 9.2(4), and 9.3 before 9.3(3) allows remote attackers to cause a denial of service (device reload) via crafted ISAKMP UDP packets, aka Bug ID CSCus94026.	24/10/2015	7.8	CVE-2015-6327
cisco -- firesight_system_software	The policy implementation in Cisco FireSIGHT Management Center 5.3.1.7, 5.4.0.4, and 6.0.0 for VMware allows remote authenticated administrators to bypass intended policy restrictions and execute Linux commands as root via unspecified vectors, aka Bug ID CSCuw12839.	24/10/2015	9.0	CVE-2015-6335
ininet_solutions -- scada_web_server	Multiple stack-based buffer overflows in IniNet embeddedWebServer (aka eWebServer) before 2.02 allow remote attackers to execute arbitrary code via a long field in an HTTP request.	24/10/2015	10.0	CVE-2015-1001
apple -- mac_os_x	The kernel in Apple OS X before 10.11.1 allows local users to gain privileges by leveraging an unspecified "type confusion" during Mach task processing.	23/10/2015	7.2	CVE-2015-5932
apple -- mac_os_x	The Sandbox subsystem in Apple OS X before 10.11.1 allows local users to gain privileges via vectors involving NVRAM parameters.	23/10/2015	7.2	CVE-2015-5945
apple -- iphone_os	IOHIDFamily in Apple iOS before 9.1, OS X before 10.11.1, and watchOS before 2.0.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	23/10/2015	9.3	CVE-2015-6974
apple -- iphone_os	Double free vulnerability in Apple iOS before 9.1 and OS X before 10.11.1 allows attackers to write to arbitrary files via a crafted app that accesses AtomicBufferedFile descriptors.	23/10/2015	8.8	CVE-2015-6983
apple -- mac_os_x	libarchive in Apple OS X before 10.11.1 allows attackers to write to arbitrary files via a crafted app that conducts an unspecified symlink attack.	23/10/2015	8.8	CVE-2015-6984
apple -- iphone_os	The kernel in Apple iOS before 9.1 and OS X before 10.11.1 does not initialize an unspecified data structure, which allows remote attackers to execute arbitrary code via vectors involving an unknown network-connectivity requirement.	23/10/2015	10.0	CVE-2015-6988
apple -- iphone_os	The kernel in Apple iOS before 9.1 and OS X before 10.11.1 mishandles reuse of virtual memory, which allows attackers to cause a denial of service via a crafted app.	23/10/2015	7.1	CVE-2015-6994
apple -- mac_os_x	Script Editor in Apple OS X before 10.11.1 allows remote attackers to bypass an intended user-confirmation requirement for AppleScript execution via unspecified vectors.	23/10/2015	7.5	CVE-2015-7007
apple -- mac_os_x	The MCX Application Restrictions component in Apple OS X before 10.11.1, when Managed Configuration is enabled, mishandles provisioning profiles, which allows attackers to bypass intended entitlement restrictions and gain privileges via a crafted developer-signed app.	23/10/2015	7.6	CVE-2015-7016
apple -- mac_os_x	The Graphics Drivers subsystem in Apple OS X before 10.11.1 allows local users to gain privileges or cause a denial of service (kernel memory corruption) via unspecified vectors.	23/10/2015	7.2	CVE-2015-7021

Semana 19/10/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- itunes	CoreText in Apple iOS before 9.1, OS X before 10.11.1, and iTunes before 12.3.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file, a different vulnerability than CVE-2015-6992 and CVE-2015-7017.	23/10/2015	7.5	CVE-2015-6975
apple -- iphone_os	GasGauge in Apple iOS before 9.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	23/10/2015	9.3	CVE-2015-6979
apple -- iphone_os	com.apple.driver.AppleVXD393 in the Graphics Driver subsystem in Apple iOS before 9.1 allows attackers to execute arbitrary code via a crafted app that leverages an unspecified "type confusion."	23/10/2015	9.3	CVE-2015-6986
apple -- itunes	CoreText in Apple iOS before 9.1, OS X before 10.11.1, and iTunes before 12.3.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file, a different vulnerability than CVE-2015-6975 and CVE-2015-7017.	23/10/2015	7.5	CVE-2015-6992
apple -- iphone_os	The kernel in Apple iOS before 9.1 allows attackers to cause a denial of service via a crafted app.	23/10/2015	7.1	CVE-2015-7004
apple -- itunes	CoreText in Apple iOS before 9.1, OS X before 10.11.1, and iTunes before 12.3.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file, a different vulnerability than CVE-2015-6975 and CVE-2015-6992.	23/10/2015	7.5	CVE-2015-7017
apple -- xcode	The Swift implementation in Apple Xcode before 7.1 mishandles type conversion, which has unspecified impact and attack vectors.	23/10/2015	7.5	CVE-2015-7030
apple -- mac_os_x	Apple Mac EFI before 2015-002, as used in OS X before 10.11.1 and other products, mishandles arguments, which allows attackers to reach "unused" functions via unspecified vectors.	23/10/2015	7.5	CVE-2015-7035
drupal_7_driver_for_sql_server_and_sql_azure_project -- drupal_7_driver_for_sql_server_and_sql_azure	The escapeLike function in sqlsrv/database.inc in the Drupal 7 driver for SQL Server and SQL Azure 7.x-1.x before 7.x-1.4 does not properly escape certain characters, which allows remote attackers to execute arbitrary SQL commands vectors involving a module using the db_like function.	21/10/2015	7.5	CVE-2015-7876
microsoft -- sharepoint	SQL injection vulnerability in Runtime/Runtime/AjaxCall.ashx in K2 blackpearl, smartforms, and K2 for SharePoint 4.6.7 allows remote attackers to execute arbitrary SQL commands via the xml parameter.	21/10/2015	7.5	CVE-2015-7299
oracle -- communications_applications	Unspecified vulnerability in (1) the Oracle Communications Diameter Signaling Router (DSR) component in Oracle Communications Applications 4.1.6 and earlier, 5.1.0 and earlier, 6.0.2 and earlier, and 7.1.0 and earlier; (2) the Oracle Communications Performance Intelligence Center Software component in Oracle Communications Applications 9.0.3 and earlier and 10.1.5 and earlier; (3) the Oracle Communications Policy Management component in Oracle Communications Applications 9.9.0 and earlier, 10.5.0 and earlier, 11.5.0 and earlier, and 12.1.0 and earlier; (4) the Oracle Communications Tekelec HLR Router component in Oracle Communications Applications 4.0.0; and (5) the Oracle Communications User Data Repository component in Oracle Communications Applications 10.2.0 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to PMAC.	21/10/2015	10.0	CVE-2015-2608
oracle -- database_server	Unspecified vulnerability in the Java VM component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	21/10/2015	9.0	CVE-2015-4794
oracle -- industry_applications	Unspecified vulnerability in the Oracle Utilities Work and Asset Management component in Oracle Industry Applications 1.9.1.1.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Add-On Applications.	21/10/2015	7.5	CVE-2015-4795
oracle -- database_server	Unspecified vulnerability in the Java VM component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2, when running on Windows, allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-4888.	21/10/2015	9.0	CVE-2015-4796
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Serialization.	21/10/2015	10.0	CVE-2015-4805
oracle -- mysql	Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client programs.	21/10/2015	7.2	CVE-2015-4819
oracle -- oracle_and_sun_systems_product_suite	Unspecified vulnerability in the Integrated Lights Out Manager (ILOM) component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Web.	21/10/2015	9.3	CVE-2015-4821
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2015-4881.	21/10/2015	10.0	CVE-2015-4835
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.	21/10/2015	10.0	CVE-2015-4843
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.	21/10/2015	10.0	CVE-2015-4844
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI, a different vulnerability than CVE-2015-4883.	21/10/2015	10.0	CVE-2015-4860
oracle -- database_server	Unspecified vulnerability in the Portable Clusterware component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	21/10/2015	10.0	CVE-2015-4863
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 8u60 and Java SE Embedded 8u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.	21/10/2015	7.6	CVE-2015-4868
oracle -- database_server	Unspecified vulnerability in the Database Scheduler component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Local.	21/10/2015	9.0	CVE-2015-4873
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2015-4835.	21/10/2015	10.0	CVE-2015-4881
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI, a different vulnerability than CVE-2015-4860.	21/10/2015	10.0	CVE-2015-4883
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 8u60 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to JavaFX.	21/10/2015	9.3	CVE-2015-4901
oracle -- oracle_and_sun_systems_product_suite	Unspecified vulnerability in the Integrated Lights Out Manager (ILOM) component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to System Management.	21/10/2015	10.0	CVE-2015-4915
owncloud -- owncloud	Directory traversal vulnerability in the routing component in ownCloud Server before 7.0.6 and 8.0.x before 8.0.4, when running on Windows, allows remote attackers to reinstall the application or execute arbitrary code via unspecified vectors.	21/10/2015	10.0	CVE-2015-4716
owncloud -- owncloud	The filename sanitization component in ownCloud Server before 6.0.8, 7.0.x before 7.0.6, and 8.0.x before 8.0.4 does not properly handle $_GET parameters cast by PHP to an array, which allows remote attackers to cause a denial of service (infinite loop and log file consumption) via crafted endpoint file names.	21/10/2015	7.8	CVE-2015-4717
owncloud -- owncloud	The external SMB storage driver in ownCloud Server before 6.0.8, 7.0.x before 7.0.6, and 8.0.x before 8.0.4 allows remote authenticated users to execute arbitrary SMB commands via a ; (semicolon) character in a file.	21/10/2015	9.0	CVE-2015-4718
owncloud -- owncloud	icewind1991 SMB before 1.0.3 allows remote authenticated users to execute arbitrary SMB commands via shell metacharacters in the user argument in the (1) listShares function in Server.php or the (2) connect or (3) read function in Share.php.	21/10/2015	9.0	CVE-2015-7698
accelerite -- radia_client_automation	Stack-based buffer overflow in the agent in Persistent Accelerite Radia Client Automation (formerly HP Client Automation), possibly before 9.1, allows remote attackers to execute arbitrary code by sending a large amount of data in an environment that lacks relationship-based firewalling.	19/10/2015	10.0	CVE-2015-7860
accelerite -- radia_client_automation	Persistent Accelerite Radia Client Automation (formerly HP Client Automation), possibly before 9.1, allows remote attackers to execute arbitrary code by sending unspecified commands in an environment that lacks relationship-based firewalling.	19/10/2015	10.0	CVE-2015-7861
juniper -- junos	The PFE daemon in Juniper vSRX virtual firewalls with Junos OS before 15.1X49-D20 allows remote attackers to cause a denial of service via an unspecified connection request to the "host-OS."	19/10/2015	7.8	CVE-2015-7749
juniper -- junos	The SSH server in Juniper Junos OS before 12.1X44-D50, 12.1X46 before 12.1X46-D35, 12.1X47 before 12.1X47-D25, 12.3 before 12.3R10, 12.3X48 before 12.3X48-D10, 13.2 before 13.2R8, 13.2X51 before 13.2X51-D35, 13.3 before 13.3R6, 14.1 before 14.1R5, 14.1X53 before 14.1X53-D25, 14.2 before 14.2R3, 15.1 before 15.1R1, and 15.1X49 before 15.1X49-D20 allows remote attackers to cause a denial of service (CPU consumption) via unspecified SSH traffic.	19/10/2015	7.8	CVE-2015-7752
linux -- linux_kernel	The __rds_conn_create function in net/rds/connection.c in the Linux kernel through 4.2.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound.	19/10/2015	7.8	CVE-2015-6937
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7635
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7636
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7637

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7638
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7639
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7640
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7641
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7643, and CVE-2015-7644.	18/10/2015	10.0	CVE-2015-7642
adobe -- flash_player	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7648.	18/10/2015	10.0	CVE-2015-7647
adobe -- flash_player	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7647.	18/10/2015	10.0	CVE-2015-7648
emc -- sourceone_email_supervisor	EMC SourceOne Email Supervisor before 7.2 does not properly employ random values for session IDs, which makes it easier for remote attackers to obtain access by guessing an ID.	18/10/2015	7.5	CVE-2015-6845
cloudbees -- jenkins	The API token-issuing service in CloudBees Jenkins before 1.606 and LTS before 1.596.2 allows remote attackers to gain privileges via a "forced API token change" involving anonymous users.	16/10/2015	7.5	CVE-2015-1814
juniper -- junos	Juniper Junos OS before 11.4R12-S4, 12.1X44 before 12.1X44-D41, 12.1X46 before 12.1X46-D26, 12.1X47 before 12.1X47-D11/D15, 12.2 before 12.2R9, 12.2X50 before 12.2X50-D70, 12.3 before 12.3R8, 12.3X48 before 12.3X48-D10, 12.3X50 before 12.3X50-D42, 13.1 before 13.1R4-S3, 13.1X49 before 13.1X49-D42, 13.1X50 before 13.1X50-D30, 13.2 before 13.2R6, 13.2X51 before 13.2X51-D26, 13.2X52 before 13.2X52-D15, 13.3 before 13.3R3-S3, 14.1 before 14.1R3, 14.2 before 14.2R1, 15.1 before 15.1R1, and 15.1X49 before 15.1X49-D10, when configured for IPv6, allow remote attackers to cause a denial of service (mbuf chain corruption and kernel panic) via crafted IPv6 packets.	16/10/2015	7.8	CVE-2014-6450
juniper -- junos	J-Web in Juniper vSRX virtual firewalls with Junos OS before 15.1X49-D20 allows remote attackers to cause a denial of service (system reboot) via unspecified vectors.	16/10/2015	7.8	CVE-2014-6451
opennms -- opennms	OpenNMS has a default password of rtc for the rtc account, which makes it easier for remote attackers to obtain access by leveraging knowledge of the credentials.	16/10/2015	10.0	CVE-2015-7856

Semana 12/10/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202.535 on Linux allows remote attackers to execute arbitrary code via a crafted SWF file, as exploited in the wild in October 2015.	15/10/2015	9.3	CVE-2015-7645
fortinet -- fortios	FortiOS 5.2.3, when configured to use High Availability (HA) and the dedicated management interface is enabled, does not require authentication for access to the ZebOS shell on the HA dedicated management interface, which allows remote attackers to obtain shell access via unspecified vectors.	15/10/2015	9.3	CVE-2015-7361
google -- chrome	The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.	15/10/2015	7.5	CVE-2015-6755
google -- chrome	Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.	15/10/2015	7.5	CVE-2015-6757
google -- chrome	The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.	15/10/2015	7.5	CVE-2015-6760
google -- chrome	The CSSFontFaceSrcValue::fetch function in core/css/CSSFontFaceSrcValue.cpp in the Cascading Style Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.	15/10/2015	7.5	CVE-2015-6762
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	15/10/2015	7.5	CVE-2015-6763
google -- chrome	Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	15/10/2015	7.5	CVE-2015-7834
linux -- linux_kernel	The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated by JavaScript code that creates many CANVAS elements for rendering by Chrome or Firefox.	15/10/2015	7.8	CVE-2013-7445
qnap -- qts	Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.	15/10/2015	9.3	CVE-2015-6003
sap -- hana	The hdbsql client 1.00.091.00 Build 1418659308-1530 in SAP HANA allows local users to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors, aka SAP Security Note 2140700.	15/10/2015	7.2	CVE-2015-6507
sap -- businessobjects	SAP BusinessObjects BI Platform 4.1, BusinessObjects Edge 4.0, and BusinessObjects XI (BOXI) 3.1 R3 allow remote attackers to cause a denial of service (out-of-bounds read and listener crash) via a crafted GIOP packet, aka SAP Security Note 2001108.	15/10/2015	10.0	CVE-2015-7730
solarwinds -- storage_manager	ProcessFileUpload.jsp in SolarWinds Storage Manager before 6.2 allows remote attackers to upload and execute arbitrary files via unspecified vectors.	15/10/2015	10.0	CVE-2015-7838
solarwinds -- log_and_event_manager	SolarWinds Log and Event Manager (LEM) allows remote attackers to execute arbitrary commands on managed computers via a request to services/messagebroker/nonsecurestreamingamf involving the traceroute functionality.	15/10/2015	7.5	CVE-2015-7839
solarwinds -- log_and_event_manager	The command line management console (CMC) in SolarWinds Log and Event Manager (LEM) before 6.2.0 allows remote attackers to execute arbitrary code via unspecified vectors involving the ping feature.	15/10/2015	7.5	CVE-2015-7840
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 improperly implement the Flash broker API, which has unspecified impact and attack vectors.	14/10/2015	10.0	CVE-2015-5569
adobe -- acrobat_dc	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	10.0	CVE-2015-5586
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	10.0	CVE-2015-6683
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	10.0	CVE-2015-6684
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 (memory corruption) by using the Format action for unspecified fields, a different vulnerability than CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622.	14/10/2015	9.3	CVE-2015-6685
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 (memory corruption) via a crafted set of fields, a different vulnerability than CVE-2015-6685, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622.	14/10/2015	9.3	CVE-2015-6686
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	10.0	CVE-2015-6687
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via a crafted Optional Content Groups (OCG) object in a WillSave document action, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	9.3	CVE-2015-6688
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via a crafted WillSave document action, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	9.3	CVE-2015-6689
adobe -- acrobat	Use-after-free vulnerability in the popUpMenuEx method in 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 allows attackers to execute arbitrary code via crafted arguments, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6691, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	9.3	CVE-2015-6690
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-7615, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	10.0	CVE-2015-6691
adobe -- acrobat	The signatureSetSeedValue method in 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 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted arguments, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6694, CVE-2015-6695, and CVE-2015-7622.	14/10/2015	9.3	CVE-2015-6693
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 (memory corruption) via crafted use of the fillColor attribute, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6695, and CVE-2015-7622.	14/10/2015	9.3	CVE-2015-6694
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 (memory corruption) via crafted use of the value attribute, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, and CVE-2015-7622.	14/10/2015	9.3	CVE-2015-6695
adobe -- acrobat	Heap-based buffer overflow in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6698.	14/10/2015	10.0	CVE-2015-6696

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Heap-based buffer overflow in the AcroForm implementation in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6696.	14/10/2015	9.3	CVE-2015-6698
adobe -- acrobat	The ANSendForReview method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6707
adobe -- acrobat	The ANStartApproval method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6708
adobe -- acrobat	The CBBBRInvite method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6709
adobe -- acrobat	The CBBBRInit method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6710
adobe -- acrobat	The DoIdentityDialog method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6711
adobe -- acrobat	The ANSendApprovalToAuthorEnabled method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6712
adobe -- acrobat	The Function call implementation in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6713
adobe -- acrobat	The Function bind implementation in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6714
adobe -- acrobat	The Function apply implementation in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6715
adobe -- acrobat	The ANSendForFormDistribution method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6716
adobe -- acrobat	The DynamicAnnotStore method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6717
adobe -- acrobat	The CBSharedReviewIfOfflineDialog method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6718
adobe -- acrobat	The CBSharedReviewCloseDialog method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6719
adobe -- acrobat	The ANRunSharedReviewEmailStep method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6720
adobe -- acrobat	The CBSharedReviewSecurityDialog method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6721
adobe -- acrobat	The CBSharedReviewStatusDialog method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6722

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	The ANTrustPropagateAll method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6723
adobe -- acrobat	The ANSendForApproval method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6724
adobe -- acrobat	The ANSendForSharedReview method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-6725
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 bypass JavaScript API execution restrictions and execute arbitrary commands via an app.launchURL call, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-7614
adobe -- acrobat	Use-after-free vulnerability in a SaveAs feature in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7617, and CVE-2015-7621.	14/10/2015	9.3	CVE-2015-7615
adobe -- acrobat	The ANVerifyComments method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-7616
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code by leveraging improper EScript exception handling, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, and CVE-2015-7621.	14/10/2015	9.3	CVE-2015-7617
adobe -- acrobat	The CBAutoConfigCommentRepository method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7619, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-7618
adobe -- acrobat	The ANShareFile2 method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7620, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-7619
adobe -- acrobat	The ANSendForBrowserReview method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, and CVE-2015-7623.	14/10/2015	9.3	CVE-2015-7620
adobe -- acrobat	Use-after-free vulnerability in 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 allows attackers to execute arbitrary code via a crafted U3D object, a different vulnerability than CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-7615, and CVE-2015-7617.	14/10/2015	9.3	CVE-2015-7621
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 (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-6685, CVE-2015-6686, CVE-2015-6693, CVE-2015-6694, and CVE-2015-6695.	14/10/2015	10.0	CVE-2015-7622
adobe -- acrobat	The ANAuthenticateResource method in 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 allows attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7616, CVE-2015-7618, CVE-2015-7619, and CVE-2015-7620.	14/10/2015	9.3	CVE-2015-7623
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.	14/10/2015	10.0	CVE-2015-7625
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.	14/10/2015	10.0	CVE-2015-7626
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.	14/10/2015	10.0	CVE-2015-7627
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextFormat object with a crafted tabStops property, a different vulnerability than CVE-2015-7631, CVE-2015-7643, and CVE-2015-7644.	14/10/2015	9.3	CVE-2015-7629
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7633, and CVE-2015-7634.	14/10/2015	10.0	CVE-2015-7630
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextLine object with a crafted validity property, a different vulnerability than CVE-2015-7629, CVE-2015-7643, and CVE-2015-7644.	14/10/2015	9.3	CVE-2015-7631
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Loader object with a crafted loaderBytes property.	14/10/2015	9.3	CVE-2015-7632

Histórico de vulnerabilidades de Outubro do 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7634.	14/10/2015	10.0	CVE-2015-7633
adobe -- air	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7633.	14/10/2015	10.0	CVE-2015-7634
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Video object with a crafted deblocking property, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7644.	14/10/2015	9.3	CVE-2015-7643
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7643.	14/10/2015	10.0	CVE-2015-7644
revive-adserver -- revive_adserver	Revive Adserver before 3.2.2 allows remote attackers to perform unspecified actions by leveraging an unexpired session after the user has been (1) deleted or (2) unlinked.	14/10/2015	7.5	CVE-2015-7367
revive-adserver -- revive_adserver	The default Flash cross-domain policy (crossdomain.xml) in Revive Adserver before 3.2.2 does not restrict access cross domain access, which allows remote attackers to conduct cross domain attacks via unspecified vectors.	14/10/2015	7.5	CVE-2015-7369
revive-adserver -- revive_adserver	Directory traversal vulnerability in delivery-dev/al.php in Revive Adserver before 3.2.2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the layerstyle parameter.	14/10/2015	7.5	CVE-2015-7372
microsoft -- jscript	The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted replace operation with a JavaScript regular expression, aka "Scripting Engine Memory Corruption Vulnerability."	13/10/2015	9.3	CVE-2015-2482
microsoft -- windows_10	Use-after-free vulnerability in Windows Shell 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 toolbar object, aka "Toolbar Use After Free Vulnerability."	13/10/2015	9.3	CVE-2015-2515
microsoft -- windows_7	Use-after-free vulnerability in the Tablet Input Band in Windows Shell in Microsoft Windows Vista SP2 and Windows 7 SP1 allows remote attackers to execute arbitrary code via a crafted web site, aka "Microsoft Tablet Input Band Use After Free Vulnerability."	13/10/2015	9.3	CVE-2015-2548
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 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Corruption Vulnerability."	13/10/2015	7.2	CVE-2015-2549
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 allows local users to gain privileges via a crafted application, aka "Windows Elevation of Privilege Vulnerability."	13/10/2015	7.2	CVE-2015-2550
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 mishandles junctions during mountpoint creation, which makes it easier for local users to gain privileges by leveraging certain sandbox access, aka "Windows Mount Point Elevation of Privilege Vulnerability."	13/10/2015	7.2	CVE-2015-2553
microsoft -- windows_10	The kernel in Microsoft 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 "Windows Object Reference Elevation of Privilege Vulnerability."	13/10/2015	7.2	CVE-2015-2554
microsoft -- excel	Use-after-free vulnerability in 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 2010 SP2 and 2013 SP1 allows remote attackers to execute arbitrary code via a crafted calculatedColumnFormula object in an Office document, aka "Microsoft Office Memory Corruption Vulnerability."	13/10/2015	9.3	CVE-2015-2555
microsoft -- visio	Buffer overflow in Microsoft Visio 2007 SP3 and 2010 SP2 allows remote attackers to execute arbitrary code via crafted UML data in an Office document, aka "Microsoft Office Memory Corruption Vulnerability."	13/10/2015	9.3	CVE-2015-2557
microsoft -- excel	Use-after-free vulnerability in Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Excel Viewer, Office Compatibility Pack SP3, and Excel Services on SharePoint Server 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a long fileVersion element in an Office document, aka "Microsoft Office Memory Corruption Vulnerability."	13/10/2015	9.3	CVE-2015-2558
microsoft -- internet_explorer	Use-after-free vulnerability in the CWindow object implementation in 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."	13/10/2015	9.3	CVE-2015-6042
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-2015-6049.	13/10/2015	9.3	CVE-2015-6048
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-2015-6048.	13/10/2015	9.3	CVE-2015-6049
microsoft -- internet_explorer	Microsoft Internet Explorer 10 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."	13/10/2015	9.3	CVE-2015-6050
microsoft -- jscript	The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Filter arguments, aka "Scripting Engine Memory Corruption Vulnerability."	13/10/2015	9.3	CVE-2015-6055
microsoft -- jscript	The (1) JScript and (2) VBScript engines in Microsoft Internet Explorer 9 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."	13/10/2015	9.3	CVE-2015-6056
cisco -- aironet_access_point_software	Cisco Aironet 1850 access points with software 8.1(112.4) allow local users to gain privileges via crafted CLI commands, aka Bug ID CSCuv79694.	12/10/2015	7.2	CVE-2015-6315
cybozu -- garoon	Cybozu Garoon 3.x through 3.7.5 and 4.x through 4.0.3 allows remote authenticated users to execute arbitrary PHP code via unspecified vectors, aka CyVDB-863 and CyVDB-867.	12/10/2015	8.5	CVE-2015-5646
cybozu -- garoon	The RSS Reader component in Cybozu Garoon 3.x through 3.7.5 and 4.x through 4.0.3 allows remote authenticated users to execute arbitrary PHP code via unspecified vectors, aka CyVDB-866.	12/10/2015	8.5	CVE-2015-5647
vmware -- vcenter_server	The JMX RMI service in VMware vCenter Server 5.0 before u3e, 5.1 before u3b, 5.5 before u3, and 6.0 before u1 does not restrict registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol.	12/10/2015	10.0	CVE-2015-2342
emc -- rsa_web_threat_detection	EMC RSA Web Threat Detection before 5.1 SP1 allows local users to obtain root privileges by leveraging access to a service account and writing commands to a service configuration file.	11/10/2015	7.2	CVE-2015-4548
google -- chrome	bindings/core/v8/V8DOMWrapper.h in Blink, as used in Google Chrome before 45.0.2454.101, does not perform a rethrow action to propagate information about a cross-context exception, which allows remote attackers to bypass the Same Origin Policy via a crafted HTML document containing an IFRAME element.	11/10/2015	7.5	CVE-2015-1303
google -- chrome	object-observe.js in Google V8, as used in Google Chrome before 45.0.2454.101, does not properly restrict method calls on access-checked objects, which allows remote attackers to bypass the Same Origin Policy via a (1) observe or (2) getNotifier call.	11/10/2015	7.5	CVE-2015-1304
icu_project -- international_components_for_unicode	Unspecified vulnerability in International Components for Unicode (ICU) before 53.1.0, as used in Apple OS X before 10.11 and watchOS before 2, has unknown impact and attack vectors.	09/10/2015	10.0	CVE-2015-5922

Semana 05/10/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- safari	The Safari Extensions implementation in Apple Safari before 9 does not require user confirmation before replacing an installed extension, which has unspecified impact and attack vectors.	09/10/2015	10.0	CVE-2015-5780
apple -- mac_os_x	The Intel Graphics Driver component in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5877.	09/10/2015	7.2	CVE-2015-5830
apple -- mac_os_x	The Login Window component in Apple OS X before 10.11 does not ensure that the screen is locked at the intended time, which allows physically proximate attackers to obtain access by visiting an unattended workstation.	09/10/2015	7.2	CVE-2015-5833
apple -- mac_os_x	IOHIDFamily in Apple OS X before 10.11 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	09/10/2015	9.3	CVE-2015-5866
apple -- mac_os_x	IOGraphics in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5872, CVE-2015-5873, and CVE-2015-5890.	09/10/2015	7.2	CVE-2015-5871
apple -- mac_os_x	IOGraphics in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5871, CVE-2015-5873, and CVE-2015-5890.	09/10/2015	7.2	CVE-2015-5872
apple -- mac_os_x	IOGraphics in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5871, CVE-2015-5872, and CVE-2015-5890.	09/10/2015	7.2	CVE-2015-5873
apple -- mac_os_x	The Intel Graphics Driver component in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5830.	09/10/2015	7.2	CVE-2015-5877
apple -- mac_os_x	The TLS Handshake Protocol implementation in Secure Transport in Apple OS X before 10.11 accepts a Certificate Request message within a session in which no Server Key Exchange message has been sent, which allows remote attackers to have an unspecified impact via crafted TLS data.	09/10/2015	10.0	CVE-2015-5887
apple -- mac_os_x	The Install Framework Legacy component in Apple OS X before 10.11 allows local users to obtain root privileges via vectors involving a privileged executable file.	09/10/2015	7.2	CVE-2015-5888
apple -- mac_os_x	rsh in the remote_cmds component in Apple OS X before 10.11 allows local users to obtain root privileges via vectors involving environment variables.	09/10/2015	7.2	CVE-2015-5889
apple -- mac_os_x	IOGraphics in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5871, CVE-2015-5872, and CVE-2015-5873.	09/10/2015	7.2	CVE-2015-5890
apple -- mac_os_x	The SMB implementation in the kernel in Apple OS X before 10.11 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	09/10/2015	7.2	CVE-2015-5891
apple -- mac_os_x	The protected range register in the EFI component in Apple OS X before 10.11 has an incorrect value, which allows attackers to cause a denial of service (boot failure) via a crafted app that writes to an unintended address.	09/10/2015	7.1	CVE-2015-5900
apple -- watch_os	GasGauge in Apple watchOS before 2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5919.	09/10/2015	7.2	CVE-2015-5918
apple -- watch_os	GasGauge in Apple watchOS before 2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5918.	09/10/2015	7.2	CVE-2015-5919
konicaminolta -- ftp_utility	Buffer overflow in Konica Minolta FTP Utility 1.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a long USER command.	09/10/2015	7.5	CVE-2015-7767
konicaminolta -- ftp_utility	Buffer overflow in Konica Minolta FTP Utility 1.0 allows remote attackers to execute arbitrary code via a long CWD command.	09/10/2015	7.5	CVE-2015-7768
zohocorp -- manageengine_opmanager	ZOHO ManageEngine OpManager 11.5 build 11600 and earlier uses a hardcoded password of "plugin" for the IntegrationUser account, which allows remote authenticated users to obtain administrator access by leveraging knowledge of this password.	09/10/2015	9.0	CVE-2015-7765
zohocorp -- manageengine_opmanager	PGSQL:SubmitQuery.do in ZOHO ManageEngine OpManager 11.6, 11.5, and earlier allows remote administrators to bypass SQL query restrictions via a comment in the query to api/json/admin/SubmitQuery, as demonstrated by "INSERT/**/INTO."	09/10/2015	9.0	CVE-2015-7766
cybozu -- garoon	Cybozu Garoon 3.x through 3.7.5 and 4.x through 4.0.3 mishandles authentication requests, which allows remote authenticated users to conduct LDAP injection attacks, and consequently bypass intended login restrictions or obtain sensitive information, by leveraging certain group-administration privileges.	08/10/2015	7.0	CVE-2015-5649
cisco -- vpn_client	Cisco VPN Client 5.x through 5.0.07.0440 uses weak permissions for vpnclient.ini, which allows local users to gain privileges by entering an arbitrary program name in the Command field of the ApplicationLauncher section.	06/10/2015	7.2	CVE-2015-7600
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 21335999.	06/10/2015	10.0	CVE-2015-3823
google -- android	The Runtime subsystem in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 23050463.	06/10/2015	9.3	CVE-2015-3865
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23213430.	06/10/2015	10.0	CVE-2015-3867
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23270724.	06/10/2015	10.0	CVE-2015-3868
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23036083.	06/10/2015	10.0	CVE-2015-3869
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 22771132.	06/10/2015	10.0	CVE-2015-3870
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23031033.	06/10/2015	10.0	CVE-2015-3871
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23346388.	06/10/2015	10.0	CVE-2015-3872
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 23016072, 23248776, 23247055, 22845824, 22008959, 21814993, 21048776, 20718524, 20674674, 22388975, 20674086, 21443020, and 22077698, a different vulnerability than CVE-2015-7716.	06/10/2015	10.0	CVE-2015-3873
google -- android	The Sonivox components in Android before 5.1.1 LMY48T allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 23335715, 23307276, and 23286323.	06/10/2015	10.0	CVE-2015-3874
google -- android	libutils in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted audio file, aka internal bug 22952485.	06/10/2015	10.0	CVE-2015-3875
google -- android	Skia, as used in Android before 5.1.1 LMY48T, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 20723696.	06/10/2015	10.0	CVE-2015-3877
google -- android	Media Player Framework in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, aka internal bug 23223325.	06/10/2015	9.3	CVE-2015-3879
google -- android	mediaserver in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, aka internal bugs 20731946 and 20719651, a different vulnerability than CVE-2015-7717.	06/10/2015	9.3	CVE-2015-6596
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23306638.	06/10/2015	10.0	CVE-2015-6598
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23416608.	06/10/2015	10.0	CVE-2015-6599
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 22882938.	06/10/2015	10.0	CVE-2015-6600
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 22935234.	06/10/2015	10.0	CVE-2015-6601
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23227354.	06/10/2015	10.0	CVE-2015-6603
google -- android	libstagefright in Android before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23129786.	06/10/2015	10.0	CVE-2015-6604
google -- android	The Secure Element Evaluation Kit (aka SEEK or SmartCard API) plugin in Android before 5.1.1 LMY48T allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 22301786.	06/10/2015	9.3	CVE-2015-6606
google -- android	libstagefright in Android 5.x before 5.1.1 LMY48T allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 20721050, a different vulnerability than CVE-2015-3873.	06/10/2015	10.0	CVE-2015-7716
google -- android	mediaserver in Android 5.x before 5.1.1 LMY48T and 6.0 before 2015-10-01 allows attackers to gain privileges via a crafted application, aka internal bug 19573085, a different vulnerability than CVE-2015-6596.	06/10/2015	9.3	CVE-2015-7717
anchorcms -- anchor_cms	system/session/drivers/cookie.php in Anchor CMS 0.9.x allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted serialized object in a cookie.	05/10/2015	7.5	CVE-2015-5687
arkeia -- western_digital_arkeia	The arkeiad daemon in the Arkeia Backup Agent in Western Digital Arkeia 11.0.12 and earlier allows remote attackers to bypass authentication and execute arbitrary commands via a series of crafted requests involving the ARKFS_EXEC_CMD operation.	05/10/2015	10.0	CVE-2015-7709
email-address_project -- email-address	Algorithmic complexity vulnerability in Address.pm in the Email-Address module 1.908 and earlier for Perl allows remote attackers to cause a denial of service (CPU consumption) via a crafted string containing a list of e-mail addresses in conjunction with parenthesis characters that can be associated with nested comments. NOTE: the default configuration in 1.908 mitigates this vulnerability but misparses certain realistic comments.	05/10/2015	7.8	CVE-2015-7686
freeswitch -- freeswitch	Heap-based buffer overflow in the parse_string function in libs/esl/src/esl_json.c in FreeSWITCH before 1.4.23 and 1.6.x before 1.6.2 allows remote attackers to execute arbitrary code via a trailing \u in a json string to cJSON_Parse.	05/10/2015	7.5	CVE-2015-7392

Histórico de vulnerabilidades de Outubro do 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi-project -- glpi	Unrestricted file upload in GLPI before 0.85.3 allows remote authenticated users to execute arbitrary code by adding a file with an executable extension as an attachment to a new ticket, then accessing it via a direct request to the file in files/_tmp/.	05/10/2015	9.0	CVE-2015-7684
mitsubishi_electric -- melsec_fx3g	The HTTP application on Mitsubishi Electric MELSEC FX3G PLC devices before April 2015 allows remote attackers to cause a denial of service (device outage) via a long parameter.	05/10/2015	7.8	CVE-2015-3938
python -- python	Untrusted search path vulnerability in python.exe in Python through 3.5.0 on Windows allows local users to gain privileges via a Trojan horse readline.pyd file in the current working directory. NOTE: the vendor says "It was determined that this is a longtime behavior of Python that cannot really be altered at this point."	05/10/2015	7.2	CVE-2015-5652
ibm -- qradar_security_information_and_event_manager	The xmlrpc.cgi Webmin script in IBM QRadar SIEM 7.1 MR2 before Patch 11 IF02 and 7.2.x before 7.2.5 Patch 4 allows remote authenticated users to execute arbitrary commands with root privileges via unspecified vectors.	03/10/2015	9.0	CVE-2015-2011
ibm -- qradar_security_information_and_event_manager	Unspecified vulnerability in IBM QRadar SIEM 7.1 MR2 before Patch 11 IF02 and 7.2.x before 7.2.5 Patch 4 allows remote authenticated users to execute arbitrary commands with root privileges via unknown vectors.	03/10/2015	9.0	CVE-2015-2016
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.1 MR2 before Patch 11 IF02 and 7.2.x before 7.2.5 Patch 4 allows remote authenticated users to execute arbitrary commands with root privileges by leveraging admin access.	03/10/2015	9.0	CVE-2015-4930
canarylabs -- trendweb	Buffer overflow in Canary Labs Trend Web Server before 9.5.2 allows remote attackers to execute arbitrary code via a crafted TCP packet.	02/10/2015	7.5	CVE-2015-5653