Histórico de vulnerabilidades de Mayo a Agosto del 2015

Semana 24/08/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hp -- hspa+_gobi_4g	The HP lt4112 LTE/HSPA+ Gobi 4G module with firmware before 12.500.00.15.1803 on EliteBook, ElitePad, Elite, ProBook, Spectre, ZBook, and mt41 Thin Client devices allows remote attackers to modify data or cause a denial of service, or execute arbitrary code, via unspecified vectors.	27/08/2015	7.8	CVE-2015-5368
hp -- systems_insight_manager	HP Systems Insight Manager (SIM) before 7.5.0, as used in HP Matrix Operating Environment before 7.5.0 and other products, allows local users to gain privileges, and consequently obtain sensitive information, modify data, or cause a denial of service, via unspecified vectors.	26/08/2015	7.2	CVE-2015-5402
hp -- systems_insight_manager	HP Systems Insight Manager (SIM) before 7.5.0, as used in HP Matrix Operating Environment before 7.5.0 and other products, allows remote attackers to obtain sensitive information or modify data via unspecified vectors.	26/08/2015	7.5	CVE-2015-5404
hp -- version_control_repository_manager	Buffer overflow in HP Version Control Repository Manager (VCRM) before 7.5.0 allows remote authenticated users to modify data or cause a denial of service via unspecified vectors.	26/08/2015	7.5	CVE-2015-5409
hp -- matrix_operating_environment	HP Matrix Operating Environment before 7.5.0 allows remote attackers to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2015-5428 and CVE-2015-5429.	26/08/2015	7.5	CVE-2015-5427
hp -- matrix_operating_environment	HP Matrix Operating Environment before 7.5.0 allows remote attackers to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2015-5427 and CVE-2015-5429.	26/08/2015	7.5	CVE-2015-5428
hp -- matrix_operating_environment	HP Matrix Operating Environment before 7.5.0 allows remote attackers to obtain sensitive information or modify data via unspecified vectors, a different vulnerability than CVE-2015-5427 and CVE-2015-5428.	26/08/2015	7.5	CVE-2015-5429
hp -- virtual_connect_enterprise_manager_sdk	HP Virtual Connect Enterprise Manager (VCEM) SDK before 7.5.0, as used in HP Matrix Operating Environment before 7.5.0 and other products, allows remote attackers to obtain sensitive information or modify data via unspecified vectors.	26/08/2015	7.5	CVE-2015-5432
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	24/08/2015	10.0	CVE-2015-5566
apache -- activemq	The LDAPLoginModule implementation the Java Authentication and Authorization Service (JAAS) in Apache ActiveMQ 5.x before 5.10.1 allows remote attackers to bypass authentication by logging in with an empty password and valid username, which triggers an unauthenticated bind. NOTE: this identifier has been SPLIT per ADT2 due to different vulnerability types. See CVE-2015-6524 for the use of wildcard operators in usernames.	24/08/2015	7.5	CVE-2014-3612
drupal -- drupal	SQL injection vulnerability in the SQL comment filtering system in the Database API in Drupal 7.x before 7.39 allows remote attackers to execute arbitrary SQL commands via an SQL comment.	24/08/2015	7.5	CVE-2015-6659
f5 -- big-ip_access_policy_manager	Memory leak in the virtual server component in F5 Big-IP LTM, AAM, AFM, Analytics, APM, ASM, GTM, Link Controller, and PEM 11.5.x before 11.5.1 HF10, 11.5.3 before HF1, and 11.6.0 before HF5, BIG-IQ Cloud, Device, and Security 4.4.0 through 4.5.0, and BIG-IQ ADC 4.5.0 allows remote attackers to cause a denial of service (memory consumption) via a large number of crafted ICMP packets.	24/08/2015	7.8	CVE-2015-5058
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2875.	24/08/2015	7.5	CVE-2015-5416
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2876.	24/08/2015	7.5	CVE-2015-5417
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2877.	24/08/2015	7.5	CVE-2015-5418
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2879.	24/08/2015	7.5	CVE-2015-5419
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2880.	24/08/2015	7.5	CVE-2015-5420
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2881.	24/08/2015	7.5	CVE-2015-5421
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2883.	24/08/2015	7.5	CVE-2015-5422
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2884.	24/08/2015	7.5	CVE-2015-5423
hp -- keyview	Unspecified vulnerability in HP KeyView before 10.23.0.1 and 10.24.x before 10.24.0.1 allows remote attackers to execute arbitrary code via unknown vectors, aka ZDI-CAN-2885.	24/08/2015	7.5	CVE-2015-5424
libevent_project -- libevent	Multiple integer overflows in the evbuffer API in Libevent 1.4.x before 1.4.15, 2.0.x before 2.0.22, and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via "insanely large inputs" to the (1) evbuffer_add, (2) evbuffer_expand, or (3) bufferevent_write function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier has been SPLIT per ADT3 due to different affected versions. See CVE-2015-6525 for the functions that are only affected in 2.0 and later.	24/08/2015	7.5	CVE-2014-6272
libevent_project -- libevent	Multiple integer overflows in the evbuffer API in Libevent 2.0.x before 2.0.22 and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via "insanely large inputs" to the (1) evbuffer_add, (2) evbuffer_prepend, (3) evbuffer_expand, (4) exbuffer_reserve_space, or (5) evbuffer_read function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier was SPLIT from CVE-2014-6272 per ADT3 due to different affected versions.	24/08/2015	7.5	CVE-2015-6525
polarssl -- polarssl	Memory leak in PolarSSL before 1.2.12 and 1.3.x before 1.3.9 allows remote attackers to cause a denial of service (memory consumption) via a large number of crafted X.509 certificates. NOTE: this identifier has been SPLIT per ADT3 due to different affected versions. See CVE-2014-9744 for the ClientHello message issue.	24/08/2015	7.8	CVE-2014-8628
polarssl -- polarssl	Memory leak in PolarSSL before 1.3.9 allows remote attackers to cause a denial of service (memory consumption) via a large number of ClientHello messages. NOTE: this identifier was SPLIT from CVE-2014-8628 per ADT3 due to different affected versions.	24/08/2015	7.8	CVE-2014-9744
redhat -- openshift	Red Hat OpenShift Enterprise 3.0.0.0 does not properly check permissions, which allows remote authenticated users with build permissions to execute arbitrary shell commands with root permissions on arbitrary build pods via unspecified vectors.	24/08/2015	8.5	CVE-2015-5222
actiontec -- _ncs01_firmware	Actiontec GT784WN modems with firmware before NCS01-1.0.13 have hardcoded credentials, which makes it easier for remote attackers to obtain root access by connecting to the web administration interface.	23/08/2015	8.3	CVE-2015-2904
ibm -- systems_director	IBM Systems Director 5.2.x, 6.1.x, 6.2.0.x, 6.2.1.x, 6.3.0.0, 6.3.1.x, 6.3.2.x, 6.3.3.x, 6.3.5.0, and 6.3.6.0 improperly processes events, which allows local users to gain privileges via unspecified vectors.	23/08/2015	7.2	CVE-2015-1992
mobile_devices -- c4_obd-ii_dongle_firmware	** DISPUTED ** Mobile Devices (aka MDI) C4 OBD-II dongles with firmware 2.x and 3.4.x, as used in Metromile Pulse and other products, store SSH private keys that are the same across different customers' installations, which makes it easier for remote attackers to obtain access by leveraging knowledge of a private key from another installation. NOTE: the vendor states "This was a flaw for the developer/debugging devices (again not possible in production versions)."	23/08/2015	9.0	CVE-2015-2906
mobile_devices -- c4_obd-ii_dongle_firmware	** DISPUTED ** Mobile Devices (aka MDI) C4 OBD-II dongles with firmware 2.x and 3.4.x, as used in Metromile Pulse and other products, have hardcoded SSH credentials, which makes it easier for remote attackers to obtain access by leveraging knowledge of the required username and password. NOTE: the vendor states "This was a flaw for the developer/debugging devices (again not possible in production versions)."	23/08/2015	9.0	CVE-2015-2907
mobile_devices -- c4_obd-ii_dongle_firmware	** DISPUTED ** Mobile Devices (aka MDI) C4 OBD-II dongles with firmware 2.x and 3.4.x, as used in Metromile Pulse and other products, do not validate firmware updates, which allows remote attackers to execute arbitrary code by specifying an update server. NOTE: the vendor states "This was a flaw for the developer/debugging devices, and was fixed in production version about 3 years ago."	23/08/2015	9.0	CVE-2015-2908
openbsd -- openssh	sshd in OpenSSH 6.8 and 6.9 uses world-writable permissions for TTY devices, which allows local users to cause a denial of service (terminal disruption) or possibly have unspecified other impact by writing to a device, as demonstrated by writing an escape sequence.	23/08/2015	7.2	CVE-2015-6565
apache -- tapestry	Apache Tapestry before 5.3.6 relies on client-side object storage without checking whether a client has modified an object, which allows remote attackers to cause a denial of service (resource consumption) or execute arbitrary code via crafted serialized data.	22/08/2015	7.8	CVE-2014-1972
hp -- operations_manager_i	Unspecified vulnerability in HP Operations Manager i (OMi) 9.22, 9.23, 9.24, 9.25, 10.00, and 10.01 allows remote attackers to execute arbitrary code via unknown vectors.	22/08/2015	10.0	CVE-2015-2137
hp -- centralview_credit_risk_control	HP CentralView Fraud Risk Management 11.1, 11.2, and 11.3; CentralView Revenue Leakage Control 4.1, 4.2, and 4.3; CentralView Dealer Performance Audit 2.0 and 2.1; CentralView Credit Risk Control 2.1, 2.2, and 2.3; CentralView Roaming Fraud Control 2.1, 2.2, and 2.3; and CentralView Subscription Fraud Prevention 2.0 and 2.1 allow remote attackers to obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2015-5407 and CVE-2015-5408.	22/08/2015	9.0	CVE-2015-5406

Histórico de vulnerabilidades de Mayo a Agosto del 2015

Semana 10/08/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- internet_explorer	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2452.	14/08/2015	9.3	CVE-2015-2441
microsoft -- internet_explorer	Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2444.	14/08/2015	9.3	CVE-2015-2442
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."	14/08/2015	9.3	CVE-2015-2443
microsoft -- internet_explorer	Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2442.	14/08/2015	9.3	CVE-2015-2444
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2447.	14/08/2015	9.3	CVE-2015-2446
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2446.	14/08/2015	9.3	CVE-2015-2447
microsoft -- internet_explorer	Microsoft Internet Explorer 9 and 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability."	14/08/2015	9.3	CVE-2015-2448
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2451.	14/08/2015	9.3	CVE-2015-2450
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2450.	14/08/2015	9.3	CVE-2015-2451
microsoft -- internet_explorer	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2441.	14/08/2015	9.3	CVE-2015-2452
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.	13/08/2015	10.0	CVE-2015-5125
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5127
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5541.	13/08/2015	10.0	CVE-2015-5129
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5130
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5132 and CVE-2015-5133.	13/08/2015	10.0	CVE-2015-5131
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5131 and CVE-2015-5133.	13/08/2015	10.0	CVE-2015-5132
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5131 and CVE-2015-5132.	13/08/2015	10.0	CVE-2015-5133
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5134
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5539
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5540
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5129.	13/08/2015	10.0	CVE-2015-5541
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5544
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5545
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5546
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5547
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5548
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5547, CVE-2015-5548, CVE-2015-5552, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5549
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5550
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5551

Histórico de vulnerabilidades de Mayo a Agosto del 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, and CVE-2015-5553.	13/08/2015	10.0	CVE-2015-5552
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, and CVE-2015-5552.	13/08/2015	10.0	CVE-2015-5553
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5555, CVE-2015-5558, and CVE-2015-5562.	13/08/2015	10.0	CVE-2015-5554
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5558, and CVE-2015-5562.	13/08/2015	10.0	CVE-2015-5555
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5556
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5557
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5555, and CVE-2015-5562.	13/08/2015	10.0	CVE-2015-5558
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5559
adobe -- air	Integer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors.	13/08/2015	10.0	CVE-2015-5560
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5561
adobe -- air	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5555, and CVE-2015-5558.	13/08/2015	10.0	CVE-2015-5562
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5564, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5563
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5565.	13/08/2015	10.0	CVE-2015-5564
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5564.	13/08/2015	10.0	CVE-2015-5565
apache -- groovy	The MethodClosure class in runtime/MethodClosure.java in Apache Groovy 1.7.0 through 2.4.3 allows remote attackers to execute arbitrary code or cause a denial of service via a crafted serialized object.	13/08/2015	7.5	CVE-2015-3253
belkin -- n300_dual-band_wi-fi_range_extender_firmware	Belkin N300 Dual-Band Wi-Fi Range Extender with firmware before 1.04.10 allows remote authenticated users to execute arbitrary commands via the (1) sub_dir parameter in a formUSBStorage request; pinCode parameter in a (2) formWpsStart or (3) formiNICWpsStart request; (4) wps_enrolee_pin parameter in a formWlanSetupWPS request; or unspecified parameters in a (5) formWlanMP, (6) formBSSetSitesurvey, (7) formHwSet, or (8) formConnectionSetting request.	13/08/2015	9.0	CVE-2015-5536
bittorrent -- bittorrent	BitTorrent and uTorrent allow remote attackers to inject command line parameters and execute arbitrary commands via a crafted URL using the (1) bittorrent or (2) magnet protocol.	13/08/2015	9.3	CVE-2015-5474
bittorrent -- bootstrap-dht	The lazy_bdecode function in BitTorrent DHT bootstrap server (bootstrap-dht) allows remote attackers to execute arbitrary code via a crafted packet, related to "improper indexing."	13/08/2015	7.5	CVE-2015-5685
clusterlabs -- pacemaker	Pacemaker before 1.1.13 does not properly evaluate added nodes, which allows remote read-only users to gain privileges via an acl command.	12/08/2015	7.5	CVE-2015-1867
clutter_project -- clutter	The gesture handling code in Clutter before 1.16.2 allows physically proximate attackers to bypass the lock screen via certain (1) mouse or (2) touch gestures.	12/08/2015	7.2	CVE-2015-3213
libidn_project -- libidn	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.	12/08/2015	7.5	CVE-2015-2059
xen -- xen	Heap-based buffer overflow in the IDE subsystem in QEMU, as used in Xen 4.5.x and earlier, when the container has a CDROM drive enabled, allows local guest users to execute arbitrary code on the host via unspecified ATAPI commands.	12/08/2015	7.2	CVE-2015-5154
xen -- xen	Use-after-free vulnerability in QEMU in Xen 4.5.x and earlier does not completely unplug emulated block devices, which allows local HVM guest users to gain privileges by unplugging a block device twice.	12/08/2015	7.2	CVE-2015-5166
cacti -- cacti	SQL injection vulnerability in graphs.php in Cacti before 0.8.8e allows remote attackers to execute arbitrary SQL commands via the local_graph_id parameter.	11/08/2015	7.5	CVE-2015-4634
redhat -- jboss_bpm_suite	XML external entity (XXE) vulnerability in the dashbuilder import facility (DocumentBuilders in org.jboss.dashboard.export.ImportManagerImpl) in Red Hat JBoss BPM Suite before 6.1.2 allows remote attackers to read arbitrary files, conduct server-side request forgery (SSRF) attacks, and have other unspecified impact via a crafted XML document.	11/08/2015	7.5	CVE-2015-1818
redhat -- libuser	libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, directly modifies /etc/passwd, which allows local users to cause a denial of service (inconsistent file state) by causing an error during the modification. NOTE: this issue can be combined with CVE-2015-3245 to gain privileges.	11/08/2015	7.2	CVE-2015-3246
linux -- linux_kernel	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an "I/O vector array overrun."	08/08/2015	7.2	CVE-2015-1805
sierrawireless -- aleos	Sierra Wireless ALEOS before 4.4.2 on AirLink ES, GX, and LS devices has hardcoded root accounts, which makes it easier for remote attackers to obtain administrative access via a (1) SSH or (2) TELNET session.	07/08/2015	10.0	CVE-2015-2897

Semana 03/08/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
timedoctor -- timedoctor	The autoupdate implementation in TimeDoctor Pro 1.4.72.3 on Windows relies on unsigned installer files that are retrieved without use of SSL, which makes it easier for man-in-the-middle attackers to execute arbitrary code via a crafted file.	06/08/2015	9.3	CVE-2015-4674
gehealthcare -- entegra_p&r_firmware	GE Healthcare eNTEGRA P&R has a password of (1) entegra for the entegra user, (2) passme for the super user of the Polestar/Polestar-i Starlink 4 upgrade, (3) 0 for the entegra user of the Codonics printer FTP service, (4) eNTEGRA for the eNTEGRA P&R user account, (5) insite for the WinVNC Login, and possibly other accounts, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2001-1594
gehealthcare -- millennium_mg	GE Healthcare Millennium MG, NC, and MyoSIGHT has a default password of (1) root.genie for the root user, (2) "service." for the service user, (3) admin.genie for the admin user, (4) reboot for the reboot user, and (5) shutdown for the shutdwon user, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2002-2445
gehealthcare -- millennium_mg_firmware	GE Healthcare Millennium MG, NC, and MyoSIGHT has a password of insite.genieacq for the insite account that cannot be changed without disabling product functionality for remote InSite support, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2002-2446
gehealthcare -- discovery_vh	GE Healthcare Discovery VH has a default password of (1) interfile for the ftpclient user of the Interfile server or (2) "2" for the LOCAL user of the FTP server for the Codonics printer, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2003-1603
gehealthcare -- centricity_image_vault_firmware	GE Healthcare Centricity Image Vault 3.x has a password of (1) gemnet for the administrator account, (2) webadmin for the webadmin administrator account of the ASACA DVD library, (3) an empty value for the gemsservice account of the Ultrasound Database, and possibly (4) gemnet2002 for the gemnet2002 account of the GEMNet license server, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2004-2777
gehealthcare -- infinia_ii_firmware	GE Healthcare Infinia II has a default password of (1) infinia for the infinia user, (2) #bigguy1 for the acqservice user, (3) dont4get2 for the Administrator user, (4) #bigguy1 for the emergency user, and (5) 2Bfamous for the InfiniaAdmin user, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2006-7253
gehealthcare -- centricity_dms_firmware	GE Healthcare Centricity DMS 4.2, 4.1, and 4.0 has a password of Muse!Admin for the Museadmin user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2007-6757
gehealthcare -- discovery_530c_firmware	GE Healthcare Discovery 530C has a password of #bigguy1 for the (1) acqservice user and (2) wsservice user of the Xeleris System, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2009-5143
gehealthcare -- optima_ct520_firmware	GE Healthcare Optima CT680, CT540, CT640, and CT520 has a default password of #bigguy for the root user, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2010-5306
gehealthcare -- optima_mr360_firmware	The HIPAA configuration interface in GE Healthcare Optima MR360 has a password of (1) operator for the root account, (2) adw2.0 for the admin account, and (3) adw2.0 for the sdc account, which has unspecified impact and attack vectors. NOTE: it is not clear whether these passwords are default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2010-5307
gehealthcare -- optima_mr360_firmware	GE Healthcare Optima MR360 does not require authentication for the HIPAA emergency login procedure, which allows physically proximate users to gain access via an arbitrary username in the Emergency Login screen. NOTE: this might not qualify for inclusion in CVE if unauthenticated emergency access is part of the intended security policy of the product, can be controlled by the system administrator, and is not enabled by default.	04/08/2015	10.0	CVE-2010-5308
gehealthcare -- cadstream_server_firmware	GE Healthcare CADStream Server has a default password of confirma for the admin user, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2010-5309
gehealthcare -- revolution_xq/i	The Acquisition Workstation for the GE Healthcare Revolution XQ/i has a password of adw3.1 for the sdc user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2010-5310
gehealthcare -- centricity_analytics_server	GE Healthcare Centricity Analytics Server 1.1 has a default password of (1) V0yag3r for the SQL Server sa user, (2) G3car3s for the analyst user, (3) G3car3s for the ccg user, (4) V0yag3r for the viewer user, and (5) geservice for the geservice user in the Webmin interface, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2011-5322
gehealthcare -- centricity_pacs-iw	GE Healthcare Centricity PACS-IW 3.7.3.7, 3.7.3.8, and possibly other versions has a password of A11enda1e for the sa SQL server user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2011-5323
gehealthcare -- centricity_pacs-iw	The TeraRecon server, as used in GE Healthcare Centricity PACS-IW 3.7.3.7, 3.7.3.8, and possibly other versions, has a password of (1) shared for the shared user and (2) scan for the scan user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2011-5324
gehealthcare -- precision_mpi	GE Healthcare Precision MPi has a password of (1) orion for the serviceapp user, (2) orion for the clinical operator user, and (3) PlatinumOne for the administrator user, which has unspecified impact and attack vectors. NOTE: it is not clear whether these passwords are default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2012-6660
gehealthcare -- centricity_pacs_server	GE Healthcare Centricity PACS 4.0 Server has a default password of (1) nasro for the nasro (ReadOnly) user and (2) nasrw for the nasrw (Read/Write) user, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2012-6693
gehealthcare -- centricity_pacs_server	GE Healthcare Centricity PACS Workstation 4.0 and 4.0.1, and Server 4.0, has a password of 2charGE for the geservice account, which has unspecified impact and attack vectors related to TimbuktuPro. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires it.	04/08/2015	10.0	CVE-2012-6694
gehealthcare -- centricity_pacs_workstation	GE Healthcare Centricity PACS Workstation 4.0 and 4.0.1 has a password of ddpadmin for the ddpadmin user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2012-6695
gehealthcare -- discovery_nm_750b	GE Healthcare Discovery NM 750b has a password of 2getin for the insite account for (1) Telnet and (2) FTP, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2013-7404
gehealthcare -- centricity_dms	The Ad Hoc Reporting feature in GE Healthcare Centricity DMS 4.2 has a password of Never!Mind for the Administrator user, which has unspecified impact and attack vectors. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2013-7405
gehealthcare -- centricity_pacs_workstation	GE Healthcare Centricity PACS Workstation 4.0 and 4.0.1 has a password of (1) CANal1 for the Administrator user and (2) iis for the IIS user, which has unspecified impact and attack vectors related to TimbuktuPro. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires it.	04/08/2015	10.0	CVE-2013-7442
gehealthcare -- discovery_xr656	GE Healthcare Discovery XR656 and XR656 G2 has a password of (1) 2getin for the insite user, (2) 4$xray for the xruser user, and (3) #superxr for the root user, which has unspecified impact and attack vectors. NOTE: it is not clear whether these passwords are default, hardcoded, or dependent on another system or product that requires a fixed value.	04/08/2015	10.0	CVE-2014-7232
gehealthcare -- precision_thunis-800+	GE Healthcare Precision THUNIS-800+ has a default password of (1) 1973 for the factory default System Utilities menu, (2) TH8740 for installation using TH8740_122_Setup.exe, (3) hrml for "Setup and Activation" using DSASetup, and (4) an empty string for Shutter Configuration, which has unspecified impact and attack vectors. NOTE: since these passwords appear to be used to access functionality during installation, this issue might not cross privilege boundaries and might not be a vulnerability.	04/08/2015	10.0	CVE-2014-7233
gehealthcare -- centricity_clinical_archive_audit_trail_repository	GE Healthcare Centricity Clinical Archive Audit Trail Repository has a default password of initinit for the (1) SSL key manager and (2) server keystore; (3) keystore_password for the server truststore; and atna for the (4) primary storage database and (5) archive storage database, which has unspecified impact and attack vectors.	04/08/2015	10.0	CVE-2014-9736
garrettcom -- magnum_10k_firmware	The firmware in MNS before 4.5.6 on Belden GarrettCom Magnum 6K and Magnum 10K switches has a hardcoded serial-console password for a privileged account, which might allow physically proximate attackers to obtain access by establishing a console session to a nonstandard installation on which this account is enabled, and leveraging knowledge of this password.	03/08/2015	7.2	CVE-2015-3959
ibm -- websphere_mq_light	IBM MQ Light before 1.0.0.2 allows remote attackers to cause a denial of service (CPU consumption) via a crafted byte sequence in authentication data.	03/08/2015	7.8	CVE-2015-1955
ibm -- websphere_mq_light	IBM MQ Light before 1.0.0.2 allows remote attackers to cause a denial of service (disk consumption) via a crafted byte sequence in authentication data, a different vulnerability than CVE-2015-1958 and CVE-2015-1987.	03/08/2015	7.8	CVE-2015-1956
ibm -- websphere_mq_light	IBM MQ Light before 1.0.0.2 allows remote attackers to cause a denial of service (disk consumption) via a crafted byte sequence in authentication data, a different vulnerability than CVE-2015-1956 and CVE-2015-1987.	03/08/2015	7.8	CVE-2015-1958
ibm -- websphere_mq_light	IBM MQ Light before 1.0.0.2 allows remote attackers to cause a denial of service (disk consumption) via a crafted byte sequence in authentication data, a different vulnerability than CVE-2015-1956 and CVE-2015-1958.	03/08/2015	7.8	CVE-2015-1987
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12.1 allows remote attackers to execute arbitrary code via a crafted packet, a different vulnerability than CVE-2015-4932, CVE-2015-4933, CVE-2015-4934, and CVE-2015-4935.	03/08/2015	10.0	CVE-2015-4931
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12.1 allows remote attackers to execute arbitrary code via a crafted packet, a different vulnerability than CVE-2015-4931, CVE-2015-4933, CVE-2015-4934, and CVE-2015-4935.	03/08/2015	10.0	CVE-2015-4932
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12.1 allows remote attackers to execute arbitrary code via a crafted packet, a different vulnerability than CVE-2015-4931, CVE-2015-4932, CVE-2015-4934, and CVE-2015-4935.	03/08/2015	10.0	CVE-2015-4933
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12.1 allows remote attackers to execute arbitrary code via a crafted packet, a different vulnerability than CVE-2015-4931, CVE-2015-4932, CVE-2015-4933, and CVE-2015-4935.	03/08/2015	10.0	CVE-2015-4934
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12.1 allows remote attackers to execute arbitrary code via a crafted packet, a different vulnerability than CVE-2015-4931, CVE-2015-4932, CVE-2015-4933, and CVE-2015-4934.	03/08/2015	10.0	CVE-2015-4935

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openbsd -- openssh	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.	02/08/2015	8.5	CVE-2015-5600
chiyutw -- bf-630	Chiyu BF-630 and BF-630W fingerprint access-control devices allow remote attackers to bypass authentication and (1) read or (2) modify (a) Voice Time Set configuration settings via a request to voice.htm or (b) UniFinger configuration settings via a request to bf.htm, a different vulnerability than CVE-2015-2871.	31/07/2015	7.5	CVE-2015-5618
cisco -- ios_xe	Cisco IOS XE 2.x before 2.4.3 and 2.5.x before 2.5.1 on ASR 1000 devices allows remote attackers to cause a denial of service (Embedded Services Processor crash) via a crafted series of fragmented (1) IPv4 or (2) IPv6 packets, aka Bug ID CSCtd72617.	31/07/2015	7.8	CVE-2015-4291
dell -- bios	The BIOS implementation on Dell Latitude, OptiPlex, Precision Mobile Workstation, and Precision Workstation Client Solutions (CS) devices with model-dependent firmware before A21 does not enforce a BIOS_CNTL locking protection mechanism upon being woken from sleep, which allows local users to conduct EFI flash attacks by leveraging console access, a similar issue to CVE-2015-3692.	31/07/2015	7.2	CVE-2015-2890
symantec -- endpoint_protection_manager	The management console in Symantec Endpoint Protection Manager (SEPM) 12.1 before 12.1-RU6-MP1 allows remote attackers to bypass authentication via a crafted password-reset action that triggers a new administrative session.	31/07/2015	7.5	CVE-2015-1486
symantec -- endpoint_protection_manager	The management console in Symantec Endpoint Protection Manager (SEPM) 12.1 before 12.1-RU6-MP1 allows remote authenticated users to gain privileges via unspecified vectors.	31/07/2015	8.5	CVE-2015-1489
symantec -- endpoint_protection_manager	Untrusted search path vulnerability in the client in Symantec Endpoint Protection 12.1 before 12.1-RU6-MP1 allows local users to gain privileges via a Trojan horse DLL in a client install package.	31/07/2015	8.5	CVE-2015-1492

Semana 27/07/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
isc -- bind	named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.	29/07/2015	7.8	CVE-2015-5477
webservice-dic -- yoyaku	Webservice-DIC yoyaku_v41 allows remote attackers to create arbitrary files, and consequently execute arbitrary code, via unspecified vectors.	29/07/2015	7.5	CVE-2015-2977
webservice-dic -- yoyaku	Webservice-DIC yoyaku_v41 allows remote attackers to execute arbitrary OS commands via unspecified vectors.	29/07/2015	7.5	CVE-2015-2979
-- ios	The TFTP server in Cisco IOS 12.2(44)SQ1, 12.2(33)XN1, 12.4(25e)JAM1, 12.4(25e)JAO5m, 12.4(23)JY, 15.0(2)ED1, 15.0(2)EY3, 15.1(3)SVF4a, and 15.2(2)JB1 and IOS XE 2.5.x, 2.6.x, 3.1.xS, 3.2.xS, 3.3.xS, 3.4.xS, and 3.5.xS before 3.6.0S; 3.1.xSG, 3.2.xSG, and 3.3.xSG before 3.4.0SG; 3.2.xSE before 3.3.0SE; 3.2.xXO before 3.3.0XO; 3.2.xSQ; 3.3.xSQ; and 3.4.xSQ allows remote attackers to cause a denial of service (device hang or reload) via multiple requests that trigger improper memory management, aka Bug ID CSCts66733.	24/07/2015	7.1	CVE-2015-0681
cisco -- application_policy_infrastructure_controller_(apic)	Cisco Application Policy Infrastructure Controller (APIC) devices with software before 1.0(3o) and 1.1 before 1.1(1j) and Nexus 9000 ACI devices with software before 11.0(4o) and 11.1 before 11.1(1j) do not properly restrict access to the APIC filesystem, which allows remote authenticated users to obtain root privileges via unspecified use of the APIC cluster-management configuration feature, aka Bug IDs CSCuu72094 and CSCuv11991.	24/07/2015	9.0	CVE-2015-4235
cisco -- unified_meetingplace_web_conferencing	The password-change feature in Cisco Unified MeetingPlace Web Conferencing before 8.5(5) MR3 and 8.6 before 8.6(2) does not check the session ID or require entry of the current password, which allows remote attackers to reset arbitrary passwords via a crafted HTTP request, aka Bug ID CSCuu51839.	24/07/2015	10.0	CVE-2015-4262

Semana 20/07/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_policy_infrastructure_controller_(apic)	Cisco Application Policy Infrastructure Controller (APIC) devices with software before 1.0(3o) and 1.1 before 1.1(1j) and Nexus 9000 ACI devices with software before 11.0(4o) and 11.x before 11.1(1j) do not properly restrict access to the APIC filesystem, which allows remote authenticated users to obtain root privileges via unspecified use of the APIC cluster-management configuration feature, aka Bug IDs CSCuu72094 and CSCuv11991.	24/07/2015	9.0	CVE-2015-4235
cisco -- unified_meetingplace_web_conferencing	The password-change feature in Cisco Unified MeetingPlace Web Conferencing 8.5 before 8.5(5) MR3 and 8.6 before 8.6(2) does not check the session ID or require entry of the current password, which allows remote attackers to reset arbitrary passwords via a crafted HTTP request, aka Bug ID CSCuu51839.	24/07/2015	10.0	CVE-2015-4262
emc -- avamar_server	Directory traversal vulnerability in EMC Avamar Server 7.x before 7.1.2 and Avamar Virtual Addition (AVE) 7.x before 7.1.2 allows remote attackers to read arbitrary files by using the Avamar Desktop/Laptop client interface to send crafted parameters.	23/07/2015	7.8	CVE-2015-4527
gemalto_safenet_luna_hsm -- -	Unspecified vulnerability on the Gemalto SafeNet Luna HSM has unknown impact and attack vectors.	22/07/2015	10.0	CVE-2015-5464
google -- chrome	Use-after-free vulnerability in the GPU process implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the continued availability of a GPUChannelHost data structure during Blink shutdown, related to content/browser/gpu/browser_gpu_channel_host_factory.cc and content/renderer/render_thread_impl.cc.	22/07/2015	7.5	CVE-2015-1272
google -- chrome	Use-after-free vulnerability in content/browser/indexed_db/indexed_db_backing_store.cc in the IndexedDB implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an abort action before a certain write operation.	22/07/2015	7.5	CVE-2015-1276
google -- chrome	Use-after-free vulnerability in the accessibility implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging lack of certain validity checks for accessibility-tree data structures.	22/07/2015	7.5	CVE-2015-1277
google -- chrome	Integer overflow in the CJBig2_Image::expand function in fxcodec/jbig2/JBig2_Image.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via large height and stride values.	22/07/2015	7.5	CVE-2015-1279
google -- chrome	SkPictureShader.cpp in Skia, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging access to a renderer process and providing crafted serialized data.	22/07/2015	7.5	CVE-2015-1280
google -- chrome	The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly check for a page's maximum number of frames, which allows remote attackers to cause a denial of service (invalid count value and use-after-free) or possibly have unspecified other impact via crafted JavaScript code that makes many createElement calls for IFRAME elements.	22/07/2015	7.5	CVE-2015-1284
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	22/07/2015	7.5	CVE-2015-1289
cisco -- videoscape_policy_resource_manager	Cisco Videoscape Policy Resource Manager (PRM) 3.5.4 allows remote attackers to cause a denial of service (CPU and memory consumption, and TCP service outage) via (1) a SYN flood or (2) another type of TCP traffic flood, aka Bug IDs CSCuu35104 and CSCuu35128.	21/07/2015	7.8	CVE-2015-4283
fca -- uconnect	Unspecified vulnerability in Uconnect 15.26.1, as used in certain Fiat Chrysler Automobiles (FCA), allows remote attackers in the same cellular network to control vehicle movement, cause human harm or physical damage, or modify dashboard settings via vectors related to modification of entertainment-system firmware and access of the CAN bus due to insufficient "Radio security protection," as demonstrated on a 2014 Jeep Cherokee Limited FWD.	21/07/2015	8.3	CVE-2015-5611
tibco -- silver_fabric_enabler_for_spotfire_webplayer	Multiple unspecified vulnerabilities in TIBCO Spotfire Client and Spotfire Web Player Client in Spotfire Analyst before 5.5.2, 6.0.x before 6.0.3, 6.5.x before 6.5.3, and 7.0.x before 7.0.1; Spotfire Analytics Platform for AWS 6.5 and 7.0.x before 7.0.1; Spotfire Automation Services before 5.5.2, 6.0.x before 6.0.3, 6.5.x before 6.5.3, and 7.0.x before 7.0.1; Spotfire Deployment Kit before 5.5.2, 6.0.x before 6.0.3, 6.5.x before 6.5.3, and 7.0.x before 7.0.1; Spotfire Desktop before 6.5.2 and 7.0.x before 7.0.1; Spotfire Desktop Language Packs 7.0.x before 7.0.1; Spotfire Professional before 5.5.2, 6.0.x before 6.0.3, 6.5.x before 6.5.3, and 7.0.x before 7.0.1; Spotfire Web Player before 5.5.2, 6.0.x before 6.0.3, 6.5.x before 6.5.3, and 7.0.x before 7.0.1; and Silver Fabric Enabler for Spotfire Web Player before 2.1.1 allow remote attackers to execute arbitrary code or obtain sensitive information via unknown vectors.	21/07/2015	7.5	CVE-2015-4554
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.	20/07/2015	10.0	CVE-2015-5124
cisco -- unified_computing_system	The Manager component in Cisco Unified Computing System (UCS) 2.2(3b) on B Blade Server devices allows local users to gain privileges for executing arbitrary CLI commands by leveraging access to the subordinate fabric interconnect, aka Bug ID CSCut32778.	20/07/2015	7.2	CVE-2015-4279
microsoft -- windows_7	Buffer underflow in atmfd.dll in the Windows Adobe Type Manager Library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code via a crafted OpenType font, aka "OpenType Font Driver Vulnerability."	20/07/2015	9.3	CVE-2015-2426
eaton -- proview	Eaton Cooper Power Systems ProView 4.0 and 5.0 before 5.0 11 on Form 6 controls and Idea and IdeaPLUS relays generates TCP initial sequence number (ISN) values linearly, which makes it easier for remote attackers to spoof TCP sessions by predicting an ISN value.	19/07/2015	9.3	CVE-2014-9196
ibm -- db2	The scalar-function implementation in IBM DB2 9.7 through FP10, 9.8 through FP5, 10.1 before FP5, and 10.5 through FP5 on Linux, UNIX, and Windows allows remote attackers to cause a denial of service or execute arbitrary code via unspecified vectors.	19/07/2015	8.0	CVE-2015-1935
sysphonic -- thetis	Multiple SQL injection vulnerabilities in Sysphonic Thetis before 2.3.0 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	19/07/2015	7.5	CVE-2015-2972
siemens -- siprotec_firmware	The EN100 module with firmware before 4.25 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service via crafted packets on UDP port 50000.	18/07/2015	7.8	CVE-2015-5374
nvidia -- gpu_driver	The NVIDIA GPU driver for FreeBSD R352 before 352.09, 346 before 346.72, R349 before 349.16, R343 before 343.36, R340 before 340.76, R337 before 337.25, R334 before 334.21, R331 before 331.113, and R304 before 304.125 allows local users with certain permissions to read or write arbitrary kernel memory via unspecified vectors that trigger an untrusted pointer dereference.	17/07/2015	7.2	CVE-2015-3625

Semana 13/07/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- videoscape_distribution_suite_for_internet_streaming	Cisco Videoscape Distribution Suite Service Broker (aka VDS-SB), when a VDSM configuration on UCS is used, and Videoscape Distribution Suite for Internet Streaming (aka VDS-IS or CDS-IS) before 3.3.1 R7 and 4.x before 4.0.0 R4 allow remote attackers to cause a denial of service (device reload) via a crafted HTTP request, aka Bug IDs CSCus79834 and CSCuu63409.	16/07/2015	7.8	CVE-2015-0725
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2015-4732.	16/07/2015	10.0	CVE-2015-2590
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Access Manager component in Oracle Fusion Middleware 11.1.2.2 allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Configuration Service.	16/07/2015	7.1	CVE-2015-2593
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 7u80 and 8u45 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Install.	16/07/2015	7.2	CVE-2015-2597
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator , a different vulnerability than CVE-2015-2603, CVE-2015-2604, CVE-2015-2605, CVE-2015-2606, and CVE-2015-4745.	16/07/2015	7.5	CVE-2015-2602
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator, a different vulnerability than CVE-2015-2602, CVE-2015-2604, CVE-2015-2605, CVE-2015-2606, and CVE-2015-4745.	16/07/2015	7.5	CVE-2015-2603
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator, a different vulnerability than CVE-2015-2602, CVE-2015-2603, CVE-2015-2605, CVE-2015-2606, and CVE-2015-4745.	16/07/2015	7.5	CVE-2015-2604
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator, a different vulnerability than CVE-2015-2602, CVE-2015-2603, CVE-2015-2604, CVE-2015-2606, and CVE-2015-4745.	16/07/2015	7.5	CVE-2015-2605
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator, a different vulnerability than CVE-2015-2602, CVE-2015-2603, CVE-2015-2604, CVE-2015-2605, and CVE-2015-4745.	16/07/2015	7.5	CVE-2015-2606
oracle -- jdk	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA.	16/07/2015	10.0	CVE-2015-2628
oracle -- database_server	Unspecified vulnerability in the Java VM component in Oracle Database Server 11.1.0.7, 11.2.0.3, 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.	16/07/2015	9.0	CVE-2015-2629
oracle -- solaris	Unspecified vulnerability in Oracle Sun Solaris 10 and 11.2 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to rmformat.	16/07/2015	7.2	CVE-2015-2631
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Data Integrator component in Oracle Fusion Middleware 11.1.1.3.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Data Quality based on Trillium, a different vulnerability than CVE-2015-0443, CVE-2015-0444, CVE-2015-0445, CVE-2015-0446, CVE-2015-2634, CVE-2015-2635, CVE-2015-4758, and CVE-2015-4759.	16/07/2015	7.5	CVE-2015-2636
oracle -- javafx	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45; JavaFX 2.2.80; and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.	16/07/2015	10.0	CVE-2015-2638
oracle -- supply_chain_products_suite	Unspecified vulnerability in the Oracle Transportation Management component in Oracle Supply Chain Products Suite 6.1, 6.2, and 6.3.0 through 6.3.7 allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Business Process Automation.	16/07/2015	7.5	CVE-2015-2663
oracle -- fusion_middleware	Unspecified vulnerability in the Oracle Endeca Information Discovery Studio component in Oracle Fusion Middleware 2.2.2, 2.3, 2.4, 3.0, and 3.1 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Integrator, a different vulnerability than CVE-2015-2602, CVE-2015-2603, CVE-2015-2604, CVE-2015-2605, and CVE-2015-2606.	16/07/2015	7.5	CVE-2015-4745
siemens -- sicam_mic_firmware	Siemens SICAM MIC devices with firmware before 2404 allow remote attackers to bypass authentication and obtain administrative access via unspecified HTTP requests.	16/07/2015	9.3	CVE-2015-5386
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-3095
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4435
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4438
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4441
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4445
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-5090 and CVE-2015-5106.	15/07/2015	7.5	CVE-2015-4446
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4451, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4447
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-4448
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4452, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4451
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-5085, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-4452

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, and CVE-2015-5086.	15/07/2015	10.0	CVE-2015-5085
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass JavaScript API execution restrictions via unspecified vectors, a different vulnerability than CVE-2015-4435, CVE-2015-4438, CVE-2015-4441, CVE-2015-4445, CVE-2015-4447, CVE-2015-4451, CVE-2015-4452, and CVE-2015-5085.	15/07/2015	10.0	CVE-2015-5086
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5087
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-4446 and CVE-2015-5106.	15/07/2015	7.5	CVE-2015-5090
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to cause a denial of service via invalid data.	15/07/2015	7.8	CVE-2015-5091
adobe -- acrobat	Buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	15/07/2015	10.0	CVE-2015-5093
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5094
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-5095
adobe -- acrobat	Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5098 and CVE-2015-5105.	15/07/2015	10.0	CVE-2015-5096
adobe -- acrobat	Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5108 and CVE-2015-5109.	15/07/2015	10.0	CVE-2015-5097
adobe -- acrobat	Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5096 and CVE-2015-5105.	15/07/2015	10.0	CVE-2015-5098
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5101, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-5099
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5102, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5100
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5111, CVE-2015-5113, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-5101
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5103, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5102
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5104, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5103
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, and CVE-2015-5115.	15/07/2015	10.0	CVE-2015-5104
adobe -- acrobat	Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5096 and CVE-2015-5098.	15/07/2015	10.0	CVE-2015-5105
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allow attackers to bypass intended access restrictions and perform a transition from Low Integrity to Medium Integrity via unspecified vectors, a different vulnerability than CVE-2015-4446 and CVE-2015-5090.	15/07/2015	7.5	CVE-2015-5106
adobe -- acrobat	Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5097 and CVE-2015-5109.	15/07/2015	10.0	CVE-2015-5108
adobe -- acrobat	Integer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5097 and CVE-2015-5108.	15/07/2015	10.0	CVE-2015-5109
adobe -- acrobat	Stack-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	15/07/2015	10.0	CVE-2015-5110
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5113, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-5111
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, and CVE-2015-5114.	15/07/2015	10.0	CVE-2015-5113

Histórico de vulnerabilidades de Mayo a Agosto del 2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4448, CVE-2015-5095, CVE-2015-5099, CVE-2015-5101, CVE-2015-5111, and CVE-2015-5113.	15/07/2015	10.0	CVE-2015-5114
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.15 and 11.x before 11.0.12, Acrobat and Acrobat Reader DC Classic before 2015.006.30060, and Acrobat and Acrobat Reader DC Continuous before 2015.008.20082 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-2015-3095, CVE-2015-5087, CVE-2015-5094, CVE-2015-5100, CVE-2015-5102, CVE-2015-5103, and CVE-2015-5104.	15/07/2015	10.0	CVE-2015-5115
adobe -- shockwave_player	Adobe Shockwave Player before 12.1.9.159 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5121.	14/07/2015	10.0	CVE-2015-5120
adobe -- shockwave_player	Adobe Shockwave Player before 12.1.9.159 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5120.	14/07/2015	10.0	CVE-2015-5121
adobe -- flash_player	Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that leverages improper handling of the opaqueBackground property, as exploited in the wild in July 2015.	14/07/2015	10.0	CVE-2015-5122
adobe -- flash_player	Use-after-free vulnerability in the BitmapData class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a ValueOf function, as exploited in the wild in July 2015.	14/07/2015	10.0	CVE-2015-5123
centreon -- centreon	SQL injection vulnerability in the isUserAdmin function in include/common/common-Func.php in Centreon (formerly Merethis Centreon) 2.5.4 and earlier allows remote attackers to execute arbitrary SQL commands via the sid parameter to include/common/XmlTree/GetXmlTree.php.	14/07/2015	7.5	CVE-2015-1560
djangoproject -- django	The session backends in Django before 1.4.21, 1.5.x through 1.6.x, 1.7.x before 1.7.9, and 1.8.x before 1.8.3 allows remote attackers to cause a denial of service (session store consumption) via multiple requests with unique session keys.	14/07/2015	7.8	CVE-2015-5143
djangoproject -- django	validators.URLValidator in Django 1.8.x before 1.8.3 allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.	14/07/2015	7.8	CVE-2015-5145
juniper -- junos	The Juniper SRX Series services gateways with Junos OS 12.1X46 before 12.1X46-D35, 12.1X47 before 12.1X47-D25, and 12.3X48 before 12.3X48-D15 do not properly implement the "set system ports console insecure" feature, which allows physically proximate attackers to gain administrative privileges by leveraging access to the console port.	14/07/2015	7.2	CVE-2015-3007
juniper -- junos	Juniper Junos OS 12.1X44 before 12.1X44-D50, 12.1X46 before 12.1X46-D35, 12.1X47 before 12.1X47-D25, 12.3 before 12.3R9, 12.3X48 before 12.3X48-D15, 13.2 before 13.2R7, 13.2X51 before 13.2X51-D35, 13.2X52 before 13.2X52-D25, 13.3 before 13.3R6, 14.1R3 before 14.1R3-S2, 14.1 before 14.1R4, 14.1X53 before 14.1X53-D12, 14.1X53 before 14.1X53-D16, 14.1X55 before 14.1X55-D25, 14.2 before 14.2R2, and 15.1 before 15.1R1 allows remote attackers to cause a denial of service (mbuf and connection consumption and restart) via a large number of requests that trigger a TCP connection to move to the LAST_ACK state when there is more data to send.	14/07/2015	7.1	CVE-2015-5358
juniper -- junos	Juniper Junos OS 12.1X44 before 12.1X44-D50, 12.1X46 before 12.1X46-D35, 12.1X47 before 12.1X47-D25, 12.3 before 12.3R9, 12.3X48 before 12.3X48-D10, 13.2 before 13.2R7, 13.3 before 13.3R5, 14.1R3 before 14.1R3-S2, 14.1 before 14.1R4, 14.2 before 14.2R2, and 15.1 before 15.1R1 allows remote attackers to cause a denial of service (NULL pointer dereference and RDP crash) via a large number of BGP-VPLS advertisements with updated BGP local preference values.	14/07/2015	7.1	CVE-2015-5359
juniper -- junos	The BFD daemon in Juniper Junos OS 12.1X44 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-D15, 13.2 before 13.2R8, 13.3 before 13.3R6, 14.1 before 14.1R5, 14.1X50 before 14.1X50-D85, 14.1X55 before 14.1X55-D20, 14.2 before 14.2R3, 15.1 before 15.1R1, and 15.1X49 before 15.1X49-D10 allows remote attackers to cause a denial of service (bfdd crash and restart) or execute arbitrary code via a crafted BFD packet.	14/07/2015	9.3	CVE-2015-5362
linuxfoundation -- cups-filters	Heap-based buffer overflow in the WriteProlog function in filter/texttopdf.c in texttopdf in cups-filters before 1.0.70 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a small line size in a print job.	14/07/2015	7.5	CVE-2015-3258
linuxfoundation -- cups-filters	Integer overflow in filter/texttopdf.c in texttopdf in cups-filters before 1.0.71 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted line size in a print job, which triggers a heap-based buffer overflow.	14/07/2015	7.5	CVE-2015-3279
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2389 and CVE-2015-2411.	14/07/2015	9.3	CVE-2015-1733
microsoft -- internet_explorer	Microsoft Internet Explorer 8 and 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2388.	14/07/2015	9.3	CVE-2015-1738
microsoft -- sql_server	Microsoft SQL Server 2008 SP3 and SP4, 2008 R2 SP2 and SP3, 2012 SP1 and SP2, and 2014, when transactional replication is configured, does not prevent use of uninitialized memory in unspecified function calls, which allows remote authenticated users to execute arbitrary code by leveraging certain permissions and making a crafted query, as demonstrated by the VIEW SERVER STATE permission, aka "SQL Server Remote Code Execution Vulnerability."	14/07/2015	7.1	CVE-2015-1762
microsoft -- sql_server	Microsoft SQL Server 2008 SP3 and SP4, 2008 R2 SP2 and SP3, 2012 SP1 and SP2, and 2014 does not prevent use of uninitialized memory in certain attempts to execute virtual functions, which allows remote authenticated users to execute arbitrary code via a crafted query, aka "SQL Server Remote Code Execution Vulnerability."	14/07/2015	8.5	CVE-2015-1763
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2401 and CVE-2015-2408.	14/07/2015	9.3	CVE-2015-1767
microsoft -- windows_8.1	Hyper-V in Microsoft Windows 8.1 and Windows Server 2012 R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS or cause a denial of service (buffer overflow) by leveraging guest OS privileges, aka "Hyper-V Buffer Overflow Vulnerability."	14/07/2015	7.2	CVE-2015-2361
microsoft -- windows_8	Hyper-V in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly initialize guest OS system data structures, which allows guest OS users to execute arbitrary code on the host OS by leveraging guest OS privileges, aka "Hyper-V System Data Structure Vulnerability."	14/07/2015	7.2	CVE-2015-2362
microsoft -- windows_2003_server	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012, and Windows RT allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	14/07/2015	7.2	CVE-2015-2363
microsoft -- windows_2003_server	The graphics component in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application that leverages an incorrect bitmap conversion, aka "Graphics Component EOP Vulnerability."	14/07/2015	7.2	CVE-2015-2364
microsoft -- windows_2003_server	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	14/07/2015	7.2	CVE-2015-2365
microsoft -- windows_7	win32k.sys in the kernel-mode drivers in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	14/07/2015	7.2	CVE-2015-2366
microsoft -- windows_2003_server	The authentication implementation in the RPC subsystem in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not prevent DCE/RPC connection reflection, which allows local users to gain privileges via a crafted application, aka "Windows RPC Elevation of Privilege Vulnerability."	14/07/2015	7.2	CVE-2015-2370
microsoft -- vbscript	vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 6 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "VBScript Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2372
microsoft -- windows_7	The Remote Desktop Protocol (RDP) server service in Microsoft Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a series of crafted packets, aka "Remote Desktop Protocol (RDP) Remote Code Execution Vulnerability."	14/07/2015	10.0	CVE-2015-2373

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Office for Mac 2011, Excel Viewer 2007 SP3, Office Compatibility Pack SP3, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, and Excel Services on SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2376
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2377
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Office for Mac 2011, and Word Viewer allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2379
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, and Word 2013 RT SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2380
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2384 and CVE-2015-2425.	14/07/2015	9.3	CVE-2015-2383
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2383 and CVE-2015-2425.	14/07/2015	9.3	CVE-2015-2384
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2390, CVE-2015-2397, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.	14/07/2015	9.3	CVE-2015-2385
microsoft -- windows_2003_server	ATMFD.DLL in the Adobe Type Manager Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "ATMFD.DLL Memory Corruption Vulnerability."	14/07/2015	7.2	CVE-2015-2387
microsoft -- internet_explorer	Microsoft Internet Explorer 8 and 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1738.	14/07/2015	9.3	CVE-2015-2388
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2411.	14/07/2015	9.3	CVE-2015-2389
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2385, CVE-2015-2397, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.	14/07/2015	9.3	CVE-2015-2390
microsoft -- internet_explorer	Microsoft Internet Explorer 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2391
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2385, CVE-2015-2390, CVE-2015-2404, CVE-2015-2406, and CVE-2015-2422.	14/07/2015	9.3	CVE-2015-2397
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2408.	14/07/2015	9.3	CVE-2015-2401
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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."	14/07/2015	9.3	CVE-2015-2403
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2406, and CVE-2015-2422.	14/07/2015	9.3	CVE-2015-2404
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2422.	14/07/2015	9.3	CVE-2015-2406
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1767 and CVE-2015-2401.	14/07/2015	9.3	CVE-2015-2408
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1733 and CVE-2015-2389.	14/07/2015	9.3	CVE-2015-2411
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2415
microsoft -- internet_explorer	JScript 9 in Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "JScript9 Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2419
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-2385, CVE-2015-2390, CVE-2015-2397, CVE-2015-2404, and CVE-2015-2406.	14/07/2015	9.3	CVE-2015-2422
microsoft -- powerpoint	Microsoft PowerPoint 2007 SP3, Word 2007 SP3, PowerPoint 2010 SP2, Word 2010 SP2, PowerPoint 2013 SP1, Word 2013 SP1, and PowerPoint 2013 RT SP1 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	14/07/2015	9.3	CVE-2015-2424
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-2383 and CVE-2015-2384.	14/07/2015	9.3	CVE-2015-2425
redcarpet_project -- redcarpet	Stack-based buffer overflow in the header_anchor function in the HTML renderer in Redcarpet before 3.3.2 allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.	14/07/2015	7.5	CVE-2015-5147
ibm -- business_process_manager	The REST API in IBM Business Process Manager (BPM) 7.5.x through 7.5.1.2, 8.0.x through 8.0.1.3, 8.5.0 through 8.5.0.1, 8.5.5 through 8.5.5.0, and 8.5.6 through 8.5.6.0 allows remote authenticated users to bypass intended access restrictions and execute arbitrary JavaScript code on the server via an unspecified API call.	13/07/2015	9.0	CVE-2015-1961
emc -- recoverpoint_for_virtual_machines	EMC RecoverPoint for Virtual Machines (VMs) 4.2 allows local users to obtain root-shell access by bypassing the Installation Manager Boxmgmt CLI interface.	10/07/2015	7.2	CVE-2015-4526
vmware -- horizon_view_client	vmware-vmx.exe in VMware Workstation 7.x through 10.x before 10.0.7 and 11.x before 11.1.1, VMware Player 5.x and 6.x before 6.0.7 and 7.x before 7.1.1, and VMware Horizon Client 5.x local-mode before 5.4.2 on Windows does not provide a valid DACL pointer during the setup of the vprintproxy.exe process, which allows host OS users to gain host OS privileges by injecting a thread.	10/07/2015	7.2	CVE-2015-3650

Semana 06/07/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- asr_5000_series_software	The boot implementation on Cisco ASR 5000 and 5500 devices with software 14.0 allows local users to execute arbitrary Linux commands by leveraging administrative privileges for storage of these commands in a Compact Flash (CF) file, aka Bug ID CSCuu75278.	10/07/2015	7.2	CVE-2015-4244
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.	09/07/2015	10.0	CVE-2015-3117
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3118
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, and CVE-2015-4433.	09/07/2015	10.0	CVE-2015-3119
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3121, CVE-2015-3122, and CVE-2015-4433.	09/07/2015	10.0	CVE-2015-3120
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3122, and CVE-2015-4433.	09/07/2015	10.0	CVE-2015-3121
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-4433.	09/07/2015	10.0	CVE-2015-3122
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.	09/07/2015	10.0	CVE-2015-3123
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3124
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-4429.	09/07/2015	7.5	CVE-2015-3126
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3127
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3128
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3129
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.	09/07/2015	10.0	CVE-2015-3130
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3131
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3132
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3134, and CVE-2015-4431.	09/07/2015	10.0	CVE-2015-3133
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-4431.	09/07/2015	10.0	CVE-2015-3134
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4432 and CVE-2015-5118.	09/07/2015	10.0	CVE-2015-3135
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3136
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-3137

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4430, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-4428
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-3126.	09/07/2015	10.0	CVE-2015-4429
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-5117.	09/07/2015	10.0	CVE-2015-4430
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-3134.	09/07/2015	10.0	CVE-2015-4431
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-5118.	09/07/2015	10.0	CVE-2015-4432
adobe -- air	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-3122.	09/07/2015	10.0	CVE-2015-4433
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-4430.	09/07/2015	10.0	CVE-2015-5117
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-4432.	09/07/2015	10.0	CVE-2015-5118
google -- v8	The Utf8DecoderBase::WriteUtf16Slow function in unicode-decoder.cc in Google V8, as used in Node.js before 0.12.6, io.js before 1.8.3 and 2.x before 2.3.3, and other products, does not verify that there is memory available for a UTF-16 surrogate pair, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted byte sequence.	09/07/2015	7.5	CVE-2015-5380
adobe -- flash_player	Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a ValueOf function, as exploited in the wild in July 2015.	08/07/2015	10.0	CVE-2015-5119
easy2map_project -- easy2map	Multiple SQL injection vulnerabilities in includes/Function.php in the Easy2Map plugin before 1.2.5 for WordPress allow remote attackers to execute arbitrary SQL commands via the mapName parameter in an e2m_img_save_map_name action to wp-admin/admin-ajax.php and other unspecified vectors.	08/07/2015	7.5	CVE-2015-4614
grandstream -- gxv3611_hd_firmware	SQL injection vulnerability on the Grandstream GXV3611_HD camera with firmware before 1.0.3.9 beta allows remote attackers to execute arbitrary SQL commands by attempting to establish a TELNET session with a crafted username.	08/07/2015	7.5	CVE-2015-2866
isc -- bind	name.c in named in ISC BIND 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2, when configured as a recursive resolver with DNSSEC validation, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) by constructing crafted zone data and then making a query for a name in that zone.	08/07/2015	7.8	CVE-2015-4620
pivotx -- pivotx	PivotX before 2.3.11 does not validate the new file extension when renaming a file with multiple extensions, which allows remote attackers to execute arbitrary code by uploading a crafted file, as demonstrated by a file named foo.php.php.	08/07/2015	7.5	CVE-2015-5457
watchguard -- xcs	SQL injection vulnerability in Watchguard XCS 9.2 and 10.0 before build 150522 allows remote attackers to execute arbitrary SQL commands via the sid cookie, as demonstrated by a request to borderpost/imp/compose.php3.	08/07/2015	7.5	CVE-2015-5452
antlabs -- inngate_ig_3.01_e	SQL injection vulnerability in main.ant in the ANTlabs InnGate firmware on IG 3100, InnGate 3.01 E, InnGate 3.10 E, InnGate 3.10 M, SG 4, and SSG 4 devices, when https is used, allows remote attackers to execute arbitrary SQL commands via the ppli parameter.	07/07/2015	7.5	CVE-2015-2849
cisco -- headend_system_release	Memory leak in Cisco Headend System Release allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors, aka Bug ID CSCus91854.	06/07/2015	7.8	CVE-2015-4230
hospira -- lifecare_pcainfusion_firmware	The Hospira LifeCare PCA Infusion System before 7.0 does not validate network traffic associated with sending a (1) drug library, (2) software update, or (3) configuration change, which allows remote attackers to modify settings or medication data via packets on the (a) TELNET, (b) HTTP, (c) HTTPS, or (d) UPNP port. NOTE: this issue might overlap CVE-2015-3459.	06/07/2015	9.3	CVE-2014-5406
hospira -- lifecare_pcainfusion_firmware	Stack-based buffer overflow in Hospira LifeCare PCA Infusion System 5.0 and earlier, and possibly other versions, allows remote attackers to execute arbitrary code via unspecified vectors.	06/07/2015	10.0	CVE-2015-3955
hospira -- lifecare_pcainfusion_firmware	Hospira LifeCare PCA Infusion System 5.0 and earlier, and possibly other versions, allows remote attackers to cause a denial of service (forced manual reboot) via a flood of TCP packets.	06/07/2015	7.8	CVE-2015-3958
hp -- hp-ux	Unspecified vulnerability in pppoec in HP HP-UX 11iv2 and 11iv3 allows local users to gain privileges by leveraging setuid permissions.	06/07/2015	7.2	CVE-2015-2126
panasonic -- security_api_activex_sdk	Stack-based buffer overflow in the Ipropsapi.ipropsapiCtrl.1 ActiveX control in ipropsapivideo in Panasonic Security API (PS-API) ActiveX SDK before 8.10.18 allows remote attackers to execute arbitrary code via a long string to the MulticastAddr method.	06/07/2015	7.5	CVE-2015-4648
samsung -- galaxy_s5	The createFromParcel method in the com.absolute.android.persistence.MethodSpec class in Samsung Galaxy S5s allows remote attackers to execute arbitrary files via a crafted Parcelable object in a serialized MethodSpec object.	06/07/2015	7.9	CVE-2015-4034
solarwinds -- storage_manager	The AuthenticationFilter class in SolarWinds Storage Manager allows remote attackers to upload and execute arbitrary scripts via unspecified vectors.	06/07/2015	10.0	CVE-2015-5371
emc -- secure_remote_services	EMC Secure Remote Services Virtual Edition (ESRS VE) 3.x before 3.06 does not properly generate random values for session cookies, which makes it easier for remote attackers to hijack sessions by predicting a value.	05/07/2015	9.3	CVE-2015-0544
mozilla -- firefox	Use-after-free vulnerability in the CanonicalizeXPCOMParticipant function in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 allows remote attackers to execute arbitrary code via vectors involving attachment of an XMLHttpRequest object to a shared worker.	05/07/2015	10.0	CVE-2015-2722
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	05/07/2015	10.0	CVE-2015-2724
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	05/07/2015	10.0	CVE-2015-2725
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	05/07/2015	10.0	CVE-2015-2726
mozilla -- firefox	The IndexedDatabaseManager class in the IndexedDB implementation in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 misinterprets an unspecified IDBDatabase field as a pointer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors, related to a "type confusion" issue.	05/07/2015	7.5	CVE-2015-2728
mozilla -- firefox	Use-after-free vulnerability in the CSPService::ShouldLoad function in the microtask implementation in Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 allows remote attackers to execute arbitrary code by leveraging client-side JavaScript that triggers removal of a DOM object on the basis of a Content Policy.	05/07/2015	10.0	CVE-2015-2731

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox	Use-after-free vulnerability in the CanonicalizeXPCOMParticipant function in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 allows remote attackers to execute arbitrary code via vectors involving attachment of an XMLHttpRequest object to a dedicated worker.	05/07/2015	10.0	CVE-2015-2733
mozilla -- firefox	The CairoTextureClientD3D9::BorrowDrawTarget function in the Direct3D 9 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.	05/07/2015	10.0	CVE-2015-2734
mozilla -- firefox	nsZipArchive.cpp in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which allows remote attackers to have an unspecified impact via a crafted ZIP archive.	05/07/2015	9.3	CVE-2015-2735
mozilla -- firefox	The nsZipArchive::BuildFileList function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which allows remote attackers to have an unspecified impact via a crafted ZIP archive.	05/07/2015	9.3	CVE-2015-2736
mozilla -- firefox	The rx::d3d11::SetBufferData function in the Direct3D 11 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.	05/07/2015	10.0	CVE-2015-2737
mozilla -- firefox	The YCbCrImageDataDeserializer::ToDataSourceSurface function in the YCbCr implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors.	05/07/2015	10.0	CVE-2015-2738
mozilla -- firefox	The ArrayBufferBuilder::append function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which has unspecified impact and attack vectors.	05/07/2015	10.0	CVE-2015-2739
mozilla -- firefox	Buffer overflow in the nsXMLHttpRequest::AppendToResponseText function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 might allow remote attackers to cause a denial of service or have unspecified other impact via unknown vectors.	05/07/2015	10.0	CVE-2015-2740
mozilla -- firefox	PDF.js in Mozilla Firefox before 39.0 and Firefox ESR 31.x before 31.8 and 38.x before 38.1 enables excessive privileges for internal Workers, which might allow remote attackers to execute arbitrary code by leveraging a Same Origin Policy bypass.	05/07/2015	7.5	CVE-2015-2743
emc -- isilon_onefs	The log-gather implementation in the web administration interface in EMC Isilon OneFS 6.5.x.x through 7.1.1.x before 7.1.1.5 and 7.2.0.x before 7.2.0.2 allows remote authenticated users to execute arbitrary commands with root privileges via unspecified vectors.	04/07/2015	9.0	CVE-2015-4525
cisco -- nx-os	Cisco NX-OS 6.0(2) and 6.2(2) on Nexus devices has an improper OS configuration, which allows local users to obtain root access via unspecified input to the Python interpreter, aka Bug IDs CSCun02887, CSCur00115, and CSCur00127.	03/07/2015	7.2	CVE-2015-4234

Semana 29/06/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
novius-os -- novius_os	Directory traversal vulnerability in Novius OS 5.0.1 (Elche) allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the tab parameter to admin/.	01/07/2015	7.5	CVE-2015-5353
cisco -- unified_ip_phones_9900_series_firmware	The packet-storing feature on Cisco 9900 phones with firmware 9.3(2) does not properly support the RTP protocol, which allows remote attackers to cause a denial of service (device hang) by sending malformed RTP packets after a call is answered, aka Bug ID CSCur39976.	30/06/2015	7.1	CVE-2015-4226
cisco -- headend_system_release	Memory leak in Cisco Headend System Release allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors, aka Bug ID CSCus91838.	30/06/2015	7.8	CVE-2015-4227
ibm -- tivoli_storage_manager_fastback	Buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	30/06/2015	7.8	CVE-2015-1923
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1924
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1925
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1929
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1930
ibm -- tivoli_storage_manager_fastback	The server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to execute arbitrary commands via unspecified vectors, a different vulnerability than CVE-2015-1986.	30/06/2015	10.0	CVE-2015-1938
ibm -- tivoli_storage_manager_fastback	The server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to read arbitrary files via a crafted TCP packet to an unspecified port.	30/06/2015	7.8	CVE-2015-1941
ibm -- tivoli_storage_manager_fastback	The server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to write to arbitrary files, and subsequently execute these files, via a crafted TCP packet to an unspecified port.	30/06/2015	9.3	CVE-2015-1942
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1948
ibm -- tivoli_storage_manager_fastback	The server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to execute arbitrary commands with SYSTEM privileges via unspecified vectors.	30/06/2015	10.0	CVE-2015-1949
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1953
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1962, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1954
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1963, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1962
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1964, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1963
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, and CVE-2015-1965.	30/06/2015	7.8	CVE-2015-1964
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors, a different vulnerability than CVE-2015-1924, CVE-2015-1925, CVE-2015-1929, CVE-2015-1930, CVE-2015-1948, CVE-2015-1953, CVE-2015-1954, CVE-2015-1962, CVE-2015-1963, and CVE-2015-1964.	30/06/2015	7.8	CVE-2015-1965
ibm -- tivoli_storage_manager_fastback	The server in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.12 allows remote attackers to execute arbitrary commands via unspecified vectors, a different vulnerability than CVE-2015-1938.	30/06/2015	10.0	CVE-2015-1986
livelycart -- livelycart	SQL injection vulnerability in LivelyCart 1.2.0 allows remote attackers to execute arbitrary SQL commands via the search_query parameter to product/search.	30/06/2015	7.5	CVE-2015-5148
themepunch -- showbiz_pro	The ThemePunch Slider Revolution (revslider) plugin before 3.0.96 for WordPress and Showbiz Pro plugin 1.7.1 and earlier for Wordpress does not properly restrict access to administrator AJAX functionality, which allows remote attackers to (1) upload and execute arbitrary files via an update_plugin action; (2) delete arbitrary sliders via a delete_slider action; and (3) create, (4) update, (5) import, or (6) export arbitrary sliders via unspecified vectors.	30/06/2015	7.5	CVE-2014-9735
emc -- unisphere	EMC Unisphere for VMAX 8.x before 8.0.3.4 sets up the Java Debugging Wire Protocol (JDWP) service, which allows remote attackers to execute arbitrary code via unspecified vectors.	29/06/2015	10.0	CVE-2015-0545
ibm -- infosphere_datastage	IBM InfoSphere DataStage 8.1, 8.5, 8.7, 9.1, and 11.3 through 11.3.1.2 on UNIX allows local users to write to executable files, and consequently obtain root privileges, via unspecified vectors.	29/06/2015	7.2	CVE-2015-1900
emc -- documentum_thumbnail_server	Directory traversal vulnerability in EMC Documentum Thumbnail Server 6.7SP1 before P32, 6.7SP2 before P25, 7.0 before P19, 7.1 before P16, and 7.2 before P01 allows remote attackers to bypass intended Content Server access restrictions via unspecified vectors.	28/06/2015	8.5	CVE-2015-0550
cisco -- ios	Race condition in the IPv6-to-IPv4 functionality in Cisco IOS 15.3S in the Performance Routing Engine (PRE) module on UBR devices allows remote attackers to cause a denial of service (NULL pointer free and module crash) by triggering intermittent connectivity with many IPv6 CPE devices, aka Bug ID CSCug47366.	27/06/2015	7.1	CVE-2015-4199

Semana 22/06/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- wireless_lan_controller_software	Cisco Wireless LAN Controller (WLC) devices with software 7.0(240.0) allow local users to execute arbitrary OS commands in a privileged context via crafted CLI commands, aka Bug ID CSCuj39474.	26/06/2015	7.2	CVE-2015-4224
cups -- cups	The add_job function in scheduler/ipp.c in cupsd in CUPS before 2.0.3 performs incorrect free operations for multiple-value job-originating-host-name attributes, which allows remote attackers to trigger data corruption for reference-counted strings via a crafted (1) IPP_CREATE_JOB or (2) IPP_PRINT_JOB request, as demonstrated by replacing the configuration file and consequently executing arbitrary code.	26/06/2015	10.0	CVE-2015-1158
adobe -- photoshop_cc	Adobe Photoshop CC before 16.0 (aka 2015.0.0) allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	24/06/2015	10.0	CVE-2015-3109
adobe -- bridge	Integer overflow in Adobe Photoshop CC before 16.0 (aka 2015.0.0) and Adobe Bridge CC before 6.11 allows attackers to execute arbitrary code via unspecified vectors.	24/06/2015	10.0	CVE-2015-3110
adobe -- bridge	Heap-based buffer overflow in Adobe Photoshop CC before 16.0 (aka 2015.0.0) and Adobe Bridge CC before 6.11 allows attackers to execute arbitrary code via unspecified vectors.	24/06/2015	10.0	CVE-2015-3111
adobe -- bridge	Adobe Photoshop CC before 16.0 (aka 2015.0.0) and Adobe Bridge CC before 6.11 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	24/06/2015	10.0	CVE-2015-3112
cisco -- webex_meeting_center	Cisco WebEx Meeting Center does not properly restrict the content of URLs in GET requests, which allows remote attackers to obtain sensitive information or conduct SQL injection attacks via vectors involving read access to a request, aka Bug ID CSCup88398.	24/06/2015	7.5	CVE-2015-4208
cisco -- anyconnect_secure_mobility_client	Cisco AnyConnect Secure Mobility Client 3.1(60) on Windows does not properly validate pathnames, which allows local users to gain privileges via a crafted INF file, aka Bug ID CSCus65862.	24/06/2015	7.2	CVE-2015-4211
sap -- mobile_platform	XML external entity (XXE) vulnerability in SAP Mobile Platform 3 allows remote attackers to read arbitrary files or possibly have other unspecified impact via a crafted XML request, aka SAP Security Note 2159601.	24/06/2015	7.5	CVE-2015-5068
adobe -- flash_player	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows and OS X and before 11.2.202.468 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in June 2015.	23/06/2015	10.0	CVE-2015-3113
aptexx -- resident_anywhere	Aptexx Resident Anywhere does not require authentication, which allows remote attackers to obtain sensitive information or modify data via a direct request.	23/06/2015	7.5	CVE-2014-4882
audiosharescript -- audioshare	PHP remote file inclusion vulnerability in ajax/myajaxphp.php in AudioShare 2.0.2 allows remote attackers to execute arbitrary PHP code via a URL in the config['basedir'] parameter.	23/06/2015	7.5	CVE-2015-4726
avigilon -- avigilon_control_center	Directory traversal vulnerability in Avigilon Control Center (ACC) 4 before 4.12.0.54 and 5 before 5.4.2.22 allows remote attackers to read arbitrary files via a crafted help/ URL.	23/06/2015	7.8	CVE-2015-2860
cisco -- ios	Memory leak in the IPv6-to-IPv4 functionality in Cisco IOS 15.3S in the Performance Routing Engine (PRE) module on UBR devices allows remote attackers to cause a denial of service (memory consumption) by triggering an error during CPE negotiation, aka Bug ID CSCug00885.	23/06/2015	7.8	CVE-2015-4200
airties -- air_firmware	Stack-based buffer overflow in AirTies Air 6372, 5760, 5750, 5650TT, 5453, 5444TT, 5443, 5442, 5343, 5342, 5341, and 5021 DSL modems with firmware 1.0.2.0 and earlier allows remote attackers to execute arbitrary code via a long string in the redirect parameter to cgi-bin/login.	19/06/2015	10.0	CVE-2015-2797
persian_car_cms_project -- persian_car_cms	SQL injection vulnerability in Persian Car CMS 1.0 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter to the default URI.	19/06/2015	7.5	CVE-2015-4678
tinysrp_project -- tinysrp	Buffer overflow in the Tiny SRP library (aka TinySRP) allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted size value for the username field.	19/06/2015	7.5	CVE-2015-4675

Semana 15/06/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
joomla -- joomla!	SQL injection vulnerability in the EQ Event Calendar component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to eqfullevent.	18/06/2015	7.5	CVE-2015-4654
milw0rm_project -- milw0rm_clone_script	Multiple SQL injection vulnerabilities in admin/login.php in Milw0rm Clone Script 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) usr or (2) pwd parameter.	18/06/2015	7.5	CVE-2015-4658
cacti -- cacti	SQL injection vulnerability in Cacti before 0.8.8d allows remote attackers to execute arbitrary SQL commands via unspecified vectors involving a cdef id.	17/06/2015	7.5	CVE-2015-4342
cacti -- cacti	SQL injection vulnerability in the get_hash_graph_template function in lib/functions.php in Cacti before 0.8.8d allows remote attackers to execute arbitrary SQL commands via the graph_template_id parameter to graph_templates.php.	17/06/2015	7.5	CVE-2015-4454
cisco -- unified_computing_system	Cisco UCS Central Software 1.2(1a) allows local users to gain privileges for OS command execution via a crafted CLI parameter, aka Bug ID CSCut32795.	17/06/2015	7.2	CVE-2015-4183
cisco -- virtualization_experience_client_6000_series_firmware	The diagnostics subsystem in the administrative web interface on Cisco Virtualization Experience (aka VXC) Client 6215 devices with firmware 11.2(27.4) allows local users to gain privileges for OS command execution via a crafted option value, aka Bug ID CSCug54412.	17/06/2015	7.2	CVE-2015-4186
emc -- unified_infrastructure_manager/provisioning	EMC Unified Infrastructure Manager/Provisioning (UIM/P) 4.1 allows remote attackers to bypass LDAP authentication by providing a valid account name.	17/06/2015	10.0	CVE-2015-0546
frontend_user_upload_project -- frontend_user_upload	Unrestricted file upload vulnerability in the Frontend User Upload (feupload) extension 0.5.0 and earlier for TYPO3 allows remote attackers to execute arbitrary code by uploading a file with an executable extension using a frontend form, then accessing it via a direct request to the file in the fileadmin folder.	16/06/2015	7.5	CVE-2015-4607
job_fair_project -- job_fair	Unrestricted file upload vulnerability in the Job Fair (jobfair) extension before 1.0.1 for TYPO3, when using Apache with mod_mime, allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the extension upload folder.	16/06/2015	7.5	CVE-2015-4606
libmimedir_project -- libmimedir	libmimedir allows remote attackers to execute arbitrary code via a VCF file with two NULL bytes at the end of the file, related to "free" function calls in the "lexer's memory clean-up procedure."	16/06/2015	7.5	CVE-2015-3205
qemu -- qemu	Heap-based buffer overflow in the PCNET controller in QEMU allows remote attackers to execute arbitrary code by sending a packet with TXSTATUS_STARTPACKET set and then a crafted packet with TXSTATUS_DEVICEOWNS set.	15/06/2015	7.5	CVE-2015-3209
cgi_rescue -- blobee	CGI RESCUE BloBee 1.20 and earlier allows remote attackers to write to arbitrary files, and consequently execute arbitrary code, via unspecified vectors.	13/06/2015	7.5	CVE-2015-2962
igreks -- milkystep_light	Igreks MilkyStep Light 0.94 and earlier and Professional 1.82 and earlier allows remote attackers to execute arbitrary OS commands via unspecified vectors.	13/06/2015	7.5	CVE-2015-2955
igreks -- milkystep_light	SQL injection vulnerability in Igreks MilkyStep Light 0.94 and earlier and Professional 1.82 and earlier allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	13/06/2015	7.5	CVE-2015-2956
n-tron -- 702w_industrial_wireless_access_point	N-Tron 702-W Industrial Wireless Access Point devices use the same (1) SSH and (2) HTTPS private keys across different customers' installations, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of a key.	13/06/2015	8.8	CVE-2012-4716
vmware -- fusion	VMware Workstation 10.x before 10.0.5, VMware Player 6.x before 6.0.6, and VMware Fusion 6.x before 6.0.6 and 7.x before 7.0.1 allow attackers to cause a denial of service against a 32-bit guest OS or 64-bit host OS via a crafted RPC command.	13/06/2015	7.8	CVE-2015-2341
cisco -- ios_xr_software	Cisco IOS XR 4.0.1 through 4.2.0 for CRS-3 Carrier Routing System allows remote attackers to cause a denial of service (NPU ASIC scan and line-card reload) via crafted IPv6 extension headers, aka Bug ID CSCtx03546.	12/06/2015	7.8	CVE-2015-0769
cisco -- telepresence_video_communication_server_software	Cisco TelePresence Video Communication Server (VCS) X8.5RC4 allows remote attackers to cause a denial of service (CPU consumption or device outage) via a crafted SDP parameter-negotiation request in an SDP session during a SIP connection, aka Bug ID CSCut42422.	12/06/2015	7.1	CVE-2015-0772
openssl -- openssl	The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.	12/06/2015	7.5	CVE-2014-8176

Semana 08/06/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.	09/06/2015	10.0	CVE-2015-3100
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3106 and CVE-2015-3107.	09/06/2015	10.0	CVE-2015-3103
adobe -- air	Integer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.	09/06/2015	10.0	CVE-2015-3104
adobe -- air	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	09/06/2015	10.0	CVE-2015-3105
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3103 and CVE-2015-3107.	09/06/2015	10.0	CVE-2015-3106
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3103 and CVE-2015-3106.	09/06/2015	10.0	CVE-2015-3107
comodo -- geekbuddy	Comodo GeekBuddy before 4.18.121 does not restrict access to the VNC server, which allows local users to gain privileges by connecting to the server.	09/06/2015	7.2	CVE-2014-7872
microsoft -- internet_explorer	Microsoft Internet Explorer 6 through 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	09/06/2015	9.3	CVE-2015-1687
microsoft -- windows_7	Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Kernel Use After Free Vulnerability."	09/06/2015	7.2	CVE-2015-1720
microsoft -- windows_7	The kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a crafted application, aka "Win32k Null Pointer Dereference Vulnerability."	09/06/2015	7.2	CVE-2015-1721
microsoft -- windows_7	Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Kernel Bitmap Handling Use After Free Vulnerability."	09/06/2015	7.2	CVE-2015-1722
microsoft -- windows_7	Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Station Use After Free Vulnerability."	09/06/2015	7.2	CVE-2015-1723
microsoft -- windows_7	Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Kernel Object Use After Free Vulnerability."	09/06/2015	7.2	CVE-2015-1724
microsoft -- windows_7	Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Win32k Buffer Overflow Vulnerability."	09/06/2015	7.2	CVE-2015-1725
microsoft -- windows_7	Use-after-free vulnerability in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Microsoft Windows Kernel Brush Object Use After Free Vulnerability."	09/06/2015	7.2	CVE-2015-1726
microsoft -- windows_7	Buffer overflow in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges via a crafted application, aka "Win32k Pool Buffer Overflow Vulnerability."	09/06/2015	7.2	CVE-2015-1727
microsoft -- windows_media_player	Microsoft Windows Media Player 10 through 12 allows remote attackers to execute arbitrary code via a crafted DataObject on a web site, aka "Windows Media Player RCE via DataObject Vulnerability."	09/06/2015	9.3	CVE-2015-1728
microsoft -- internet_explorer	Microsoft Internet Explorer 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	09/06/2015	9.3	CVE-2015-1730
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1736, CVE-2015-1737, and CVE-2015-1755.	09/06/2015	9.3	CVE-2015-1731
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1742, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.	09/06/2015	9.3	CVE-2015-1732
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1740, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.	09/06/2015	9.3	CVE-2015-1735
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1737, and CVE-2015-1755.	09/06/2015	9.3	CVE-2015-1736
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1755.	09/06/2015	9.3	CVE-2015-1737
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1735, CVE-2015-1744, CVE-2015-1745, and CVE-2015-1766.	09/06/2015	9.3	CVE-2015-1740
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1752.	09/06/2015	9.3	CVE-2015-1741
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1747, CVE-2015-1750, and CVE-2015-1753.	09/06/2015	9.3	CVE-2015-1742
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1735, CVE-2015-1740, CVE-2015-1745, and CVE-2015-1766.	09/06/2015	9.3	CVE-2015-1744
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1766.	09/06/2015	9.3	CVE-2015-1745
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1750, and CVE-2015-1753.	09/06/2015	9.3	CVE-2015-1747
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1753.	09/06/2015	9.3	CVE-2015-1750
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."	09/06/2015	9.3	CVE-2015-1751

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1741.	09/06/2015	9.3	CVE-2015-1752
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1732, CVE-2015-1742, CVE-2015-1747, and CVE-2015-1750.	09/06/2015	9.3	CVE-2015-1753
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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."	09/06/2015	9.3	CVE-2015-1754
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1731, CVE-2015-1736, and CVE-2015-1737.	09/06/2015	9.3	CVE-2015-1755
microsoft -- windows_7	Use-after-free vulnerability in Microsoft Common Controls 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, and Windows RT Gold and 8.1 allows user-assisted remote attackers to execute arbitrary code via a crafted web site that is accessed with the F12 Developer Tools feature of Internet Explorer, aka "Microsoft Common Control Use After Free Vulnerability."	09/06/2015	9.3	CVE-2015-1756
microsoft -- office_compatibility_pack	Microsoft Office Compatibility Pack SP3 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/06/2015	9.3	CVE-2015-1759
microsoft -- office	Microsoft Office Compatibility Pack SP3, Office 2010 SP2, Office 2013 SP1, and Office 2013 RT SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/06/2015	9.3	CVE-2015-1760
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1735, CVE-2015-1740, CVE-2015-1744, and CVE-2015-1745.	09/06/2015	9.3	CVE-2015-1766
microsoft -- windows_2003_server	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka "Win32k Memory Corruption Elevation of Privilege Vulnerability."	09/06/2015	7.2	CVE-2015-1768
microsoft -- office_2013	Microsoft Office 2013 SP1 and 2013 RT SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Uninitialized Memory Use Vulnerability."	09/06/2015	9.3	CVE-2015-1770
microsoft -- windows_7	win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2003 SP2 and R2 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	09/06/2015	7.2	CVE-2015-2360
montala -- resourcespace	Directory traversal vulnerability in pages/setup.php in Montala Limited ResourceSpace before 7.2.6727 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the defaultlanguage parameter.	09/06/2015	7.5	CVE-2015-3648
php -- php	The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.	09/06/2015	7.5	CVE-2015-3307
php -- php	Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.	09/06/2015	7.5	CVE-2015-3329
php -- php	Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.	09/06/2015	7.5	CVE-2015-4022
php -- php	PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.	09/06/2015	7.5	CVE-2015-4025
php -- php	The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.	09/06/2015	7.5	CVE-2015-4026
php -- php	The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.	09/06/2015	7.5	CVE-2015-4147
pivotal_software -- redis	Redis before 2.8.1 and 3.x before 3.0.2 allows remote attackers to execute arbitrary Lua bytecode via the eval command.	09/06/2015	10.0	CVE-2015-4335
usersultra -- usersultra	Multiple SQL injection vulnerabilities in the ratings module in the Users Ultra plugin before 1.5.16 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) data_target or (2) data_vote parameter in a rating_vote (wp_ajax_nopriv_rating_vote) action to wp-admin/admin-ajax.php.	09/06/2015	7.5	CVE-2015-4109
beckhoff -- ipc_diagnostics	Beckhoff IPC Diagnostics before 1.8 does not properly restrict access to functions in /config, which allows remote attackers to cause a denial of service (reboot or shutdown), create arbitrary users, or possibly have unspecified other impact via a crafted request, as demonstrated by a beckhoff.com:service:cxconfig:1#Write SOAP action to /upnpisapi.	08/06/2015	9.0	CVE-2015-4051
buffalotech -- bhr-4grv2_firmware	The Buffalo WHR-1166DHP 1.60 and earlier, WSR-600DHP 1.60 and earlier, WHR-600D 1.60 and earlier, WHR-300HP2 1.60 and earlier, WMR-300 1.60 and earlier, WEX-300 1.60 and earlier, and BHR-4GRV2 1.04 and earlier routers allow remote authenticated users to execute arbitrary OS commands via unspecified vectors.	08/06/2015	7.7	CVE-2014-9284
sybase -- adaptive_server_enterprise	SAP Adaptive Server Enterprise (ASE) before 15.7 SP132 and 16.0 before 16.0 SP01 allows remote attackers to bypass the challenge and response mechanism and obtain access to the probe account via a crafted response, aka SAP Security Note 2113995.	08/06/2015	7.5	CVE-2014-6284
sysaid -- sysaid	SysAid Help Desk before 15.2 does not properly restrict access to certain functionality, which allows remote attackers to (1) create administrator accounts via a crafted request to /createnewaccount or (2) write to arbitrary files via the fileName parameter to /userentry.	08/06/2015	7.5	CVE-2015-2993
sysaid -- sysaid	Multiple directory traversal vulnerabilities in SysAid Help Desk before 15.2 allow remote attackers to (1) read arbitrary files via a .. (dot dot) in the fileName parameter to getGfiUpgradeFile or (2) cause a denial of service (CPU and memory consumption) via a .. (dot dot) in the fileName parameter to calculateRdsFileChecksum.	08/06/2015	8.5	CVE-2015-2996
sysaid -- sysaid	SysAid Help Desk before 15.2 allows remote attackers to cause a denial of service (CPU and memory consumption) via a large number of nested entity references in an XML document to (1) /agententry, (2) /rdsmonitoringresponse, or (3) /androidactions, aka an XML Entity Expansion (XEE) attack.	08/06/2015	7.8	CVE-2015-3000
t1utils_project -- t1utils	Buffer overflow in the set_cs_start function in t1disasm.c in t1utils before 1.39 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.	08/06/2015	7.5	CVE-2015-3905
zohocorp -- manageengine_netflow_analyzer	Zoho NetFlow Analyzer build 10250 and earlier does not check for administrative authorization, which allows remote attackers to obtain sensitive information, modify passwords, or remove accounts by leveraging the guest role.	08/06/2015	7.5	CVE-2015-2959
apache -- tomcat	Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (memory consumption) via a series of aborted upload attempts.	07/06/2015	7.8	CVE-2014-0230
cisco -- edge_340_firmware	Cisco Edge 300 software 1.0 and 1.1 on Edge 340 devices allows local users to obtain root privileges via unspecified commands, aka Bug ID CSCur18132.	07/06/2015	7.2	CVE-2015-0767
linux -- linux_kernel	Integer signedness error in the oz_hcd_get_desc_cnf function in drivers/staging/ozwpan/ozhcd.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted packet.	07/06/2015	9.0	CVE-2015-4001
linux -- linux_kernel	drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 does not ensure that certain length values are sufficiently large, which allows remote attackers to cause a denial of service (system crash or large loop) or possibly execute arbitrary code via a crafted packet, related to the (1) oz_usb_rx and (2) oz_usb_handle_ep_data functions.	07/06/2015	9.0	CVE-2015-4002
linux -- linux_kernel	The oz_usb_handle_ep_data function in drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via a crafted packet.	07/06/2015	7.8	CVE-2015-4003
linux -- linux_kernel	The OZWPAN driver in the Linux kernel through 4.0.5 relies on an untrusted length field during packet parsing, which allows remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read and system crash) via a crafted packet.	07/06/2015	8.5	CVE-2015-4004
novell -- zenworks_configuration_management	Directory traversal vulnerability in UploadServlet in the Remote Management component in Novell ZENworks Configuration Management (ZCM) 10 before 10.3 allows remote attackers to execute arbitrary code via a crafted WAR pathname in the filename parameter in conjunction with WAR content in the POST data, a different vulnerability than CVE-2010-5324.	07/06/2015	10.0	CVE-2010-5323
novell -- zenworks_configuration_management	Directory traversal vulnerability in UploadServlet in the Remote Management component in Novell ZENworks Configuration Management (ZCM) 10 before 10.3 allows remote attackers to execute arbitrary code via a zenworks-fileupload request with a crafted directory name in the type parameter, in conjunction with a WAR filename in the filename parameter and WAR content in the POST data, a different vulnerability than CVE-2010-5323.	07/06/2015	10.0	CVE-2010-5324
novell -- zenworks_configuration_management	Directory traversal vulnerability in UploadServlet in Novell ZENworks Configuration Management (ZCM) 10 and 11 before 11.3.2 allows remote attackers to execute arbitrary code via a crafted directory name in the uid parameter, in conjunction with a WAR filename in the filename parameter and WAR content in the POST data, a different vulnerability than CVE-2010-5323 and CVE-2010-5324.	07/06/2015	10.0	CVE-2015-0779

Semana 01/06/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- anyconnect_secure_mobility_client	Cisco AnyConnect Secure Mobility Client before 3.1(8009) and 4.x before 4.0(2052) on Linux does not properly implement unspecified internal functions, which allows local users to obtain root privileges via crafted vpnagent options, aka Bug ID CSCus86790.	04/06/2015	7.2	CVE-2015-0761
qemu -- qemu	QEMU does not properly restrict write access to the PCI config space for certain PCI pass-through devices, which mighy allow local x86 HVM guests to gain privileges, cause a denial of service (host crash), obtain sensitive information, or possibly have other unspecified impact via unknown vectors.	03/06/2015	7.2	CVE-2015-4106
xen -- xen	Xen 3.3.x through 4.5.x does not properly restrict access to PCI MSI mask bits, which allows local x86 HVM guest users to cause a denial of service (unexpected interrupt and host crash) via unspecified vectors.	03/06/2015	7.8	CVE-2015-4104
fusionforge -- fusionforge	The Git plugin for FusionForge before 6.0rc4 allows remote attackers to execute arbitrary code via an unspecified parameter when creating a secondary Git repository.	02/06/2015	10.0	CVE-2015-0850
sap -- gui	Stack-based buffer overflow in the LZC decompression implementation (CsObjectInt::CsDecomprLZC function in vpa106cslzc.cpp) in SAP MaxDB 7.5 and 7.6, Netweaver Application Server ABAP, Netweaver Application Server Java, Netweaver RFC SDK, GUI, RFC SDK, SAPCAR archive tool, and other products allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via unspecified vectors, aka SAP Security Note 2124806, 2121661, 2127995, and 2125316.	02/06/2015	7.5	CVE-2015-2282
sap -- hana_web-based_development_workbench	SQL injection vulnerability in SAP HANA Web-based Development Workbench allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Notes 2153892.	02/06/2015	7.5	CVE-2015-4159
sap -- ase_database_platform	SQL injection vulnerability in SAP ASE Database Platform allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Notes: 2152278.	02/06/2015	7.5	CVE-2015-4160
sap -- afaria	SAP Afaria does not properly restrict access to unspecified functionality, which allows remote attackers to obtain sensitive information, gain privileges, or have other unspecified impact via unknown vectors, SAP Security Note 2155690.	02/06/2015	7.5	CVE-2015-4161
netapp -- oncommand_workflow_automation	The installer in NetApp OnCommand Workflow Automation before 2.2.1P1 and 3.x before 3.0P1 sets up the Java Debugging Wire Protocol (JDWP) service, which allows remote attackers to execute arbitrary code via unspecified vectors.	31/05/2015	10.0	CVE-2015-3292
cisco -- dta_control_system	Cisco DTA Control System (DTACS) 4.0.0.9 and Cisco Headend System Release allow remote attackers to cause a denial of service (CPU and memory consumption, and TCP service outage) via (1) a SYN flood or (2) another type of TCP traffic flood, aka Bug IDs CSCus50642, CSCus50662, CSCus50625, CSCus50657, and CSCus68315.	30/05/2015	7.8	CVE-2015-0744
ibm -- powervc	IBM PowerVC 1.2.0.x through 1.2.0.4, 1.2.1.x through 1.2.1.2, and 1.2.2.x through 1.2.2.2 does not require authentication for the ceilometer NoSQL database, which allows remote attackers to read or write to arbitrary database records, and consequently obtain administrator privileges, via a session on port 27017.	30/05/2015	7.5	CVE-2015-1937
arcserve -- arcserve_unified_data_protection	Directory traversal vulnerability in Arcserve UDP before 5.0 Update 4 allows remote attackers to obtain sensitive information or cause a denial of service via a crafted file path to the (1) reportFileServlet or (2) exportServlet servlet.	29/05/2015	9.4	CVE-2015-4068
arcserve -- arcserve_unified_data_protection	The EdgeServiceImpl web service in Arcserve UDP before 5.0 Update 4 allows remote attackers to obtain sensitive credentials via a crafted SOAP request to the (1) getBackupPolicy or (2) getBackupPolicies method.	29/05/2015	7.8	CVE-2015-4069
avm -- fritz!box	AVM Fritz!Box allows remote attackers to execute arbitrary commands via shell metacharacters in the var:lang parameter to cgi-bin/webcm.	29/05/2015	10.0	CVE-2014-9727
cisco -- unified_communications_manager	Cisco IP Phone 7861, when firmware from Cisco Unified Communications Manager 10.3(1) is used, allows remote attackers to cause a denial of service via crafted packets, aka Bug ID CSCus81800.	29/05/2015	7.8	CVE-2015-0751
cisco -- finesse	Cisco Finesse 10.5(1) allows remote authenticated users to obtain sensitive information or cause a denial of service (CPU and memory consumption) via a crafted XML document, aka Bug ID CSCut95810.	29/05/2015	7.5	CVE-2015-0754
dell -- netvault_backup	Integer overflow in the libnv6 module in Dell NetVault Backup before 10.0.5 allows remote attackers to execute arbitrary code via crafted template string specifiers in a serialized object, which triggers a heap-based buffer overflow.	29/05/2015	10.0	CVE-2015-4067
ipsec-tools -- ipsec-tools	racoon/gssapi.c in IPsec-Tools 0.8.2 allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon crash) via a series of crafted UDP requests.	29/05/2015	7.8	CVE-2015-4047
milw0rm_project -- milw0rm_clone_script	SQL injection vulnerability in related.php in Milw0rm Clone Script 1.0 allows remote attackers to execute arbitrary SQL commands via the program parameter.	29/05/2015	7.5	CVE-2015-4137
visual_mining -- netcharts_server	Directory traversal vulnerability in saveFile.jsp in the development installation in Visual Mining NetChart allows remote attackers to write to arbitrary files via unspecified vectors.	29/05/2015	10.0	CVE-2015-4031
visual_mining -- netcharts_server	projectContents.jsp in the Developer tools in Visual Mining NetCharts Server allows remote attackers to rename arbitrary files, and consequently execute them, via unspecified vectors.	29/05/2015	10.0	CVE-2015-4032
wavelink -- terminal_emulation	Heap-based buffer overflow in the License Server (LicenseServer.exe) in Wavelink Terminal Emulation (TE) allows remote attackers to execute arbitrary code via a large HTTP header.	29/05/2015	10.0	CVE-2015-4059
wavelink -- connectpro	Heap-based buffer overflow in the TermProxy (WLTermProxyService.exe) service in Wavelink ConnectPro allows remote attackers to execute arbitrary code via a large HTTP header.	29/05/2015	10.0	CVE-2015-4060
wouter_verhelst -- nbd	The modern style negotiation in Network Block Device (nbd-server) 2.9.22 through 3.3 allows remote attackers to cause a denial of service (root process termination) by (1) closing the connection during negotiation or (2) specifying a name for a non-existent export.	29/05/2015	7.8	CVE-2013-7441
wouter_verhelst -- nbd	nbd-server.c in Network Block Device (nbd-server) before 3.11 does not properly handle signals, which allows remote attackers to cause a denial of service (deadlock) via unspecified vectors.	29/05/2015	7.8	CVE-2015-0847

Semana 25/05/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arubanetworks -- clearpass_policy_manager	Aruba Networks ClearPass Policy Manager (CPPM) before 6.5.0 allows remote administrators to execute arbitrary code via unspecified vectors.	28/05/2015	9.0	CVE-2014-6628
arubanetworks -- clearpass_policy_manager	Directory traversal vulnerability in Aruba Networks ClearPass Policy Manager (CPPM) before 6.4.5 allows remote administrators to execute arbitrary files via unspecified vectors.	28/05/2015	9.0	CVE-2015-1550
reflex_gallery_project -- reflex_gallery	Unrestricted file upload vulnerability in admin/scripts/FileUploader/php.php in the ReFlex Gallery plugin before 3.1.4 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a file with a PHP extension, then accessing it via a direct request to the file in uploads/ directory.	28/05/2015	7.5	CVE-2015-4133
apple -- iphone_os	CoreText in Apple iOS 8.x through 8.3 allows remote attackers to cause a denial of service (reboot and messaging disruption) via crafted Unicode text that is not properly handled during display truncation in the Notifications feature, as demonstrated by Arabic characters in (1) an SMS message or (2) a WhatsApp message.	27/05/2015	7.8	CVE-2015-1157
linux -- linux_kernel	The __driver_rfc4106_decrypt function in arch/x86/crypto/aesni-intel_glue.c in the Linux kernel before 3.19.3 does not properly determine the memory locations used for encrypted data, which allows context-dependent attackers to cause a denial of service (buffer overflow and system crash) or possibly execute arbitrary code by triggering a crypto API call, as demonstrated by use of a libkcapi test program with an AF_ALG(aead) socket.	27/05/2015	9.3	CVE-2015-3331
moxa -- vport_activex_sdk_plus	Multiple stack-based buffer overflows in Moxa VPort ActiveX SDK Plus before 2.8 allow remote attackers to insert assembly-code lines via vectors involving a regkey (1) set or (2) get command.	26/05/2015	7.5	CVE-2015-0986
sap -- sap_netweaver_application_server_java	XML external entity (XXE) vulnerability in SAP NetWeaver AS Java allows remote attackers to send TCP requests to intranet servers or possibly have other unspecified impact via an XML request, related to "CIM UPLOAD," aka SAP Security Note 2090851.	26/05/2015	7.5	CVE-2015-4091
sap -- afaria	Buffer overflow in the XComms process in SAP Afaria 7.00.6620.2 SP5 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request, aka SAP Security Note 2153690.	26/05/2015	7.5	CVE-2015-4092
wireshark -- wireshark	The dissect_lbmr_pser function in epan/dissectors/packet-lbmr.c in the LBMR dissector in Wireshark 1.12.x before 1.12.5 does not reject a zero length, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	26/05/2015	7.8	CVE-2015-3808
wireshark -- wireshark	The dissect_lbmr_pser function in epan/dissectors/packet-lbmr.c in the LBMR dissector in Wireshark 1.12.x before 1.12.5 does not properly track the current offset, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	26/05/2015	7.8	CVE-2015-3809
wireshark -- wireshark	epan/dissectors/packet-websocket.c in the WebSocket dissector in Wireshark 1.12.x before 1.12.5 uses a recursive algorithm, which allows remote attackers to cause a denial of service (CPU consumption) via a crafted packet.	26/05/2015	7.8	CVE-2015-3810
wireshark -- wireshark	Multiple memory leaks in the x11_init_protocol function in epan/dissectors/packet-x11.c in the X11 dissector in Wireshark 1.10.x before 1.10.14 and 1.12.x before 1.12.5 allow remote attackers to cause a denial of service (memory consumption) via a crafted packet.	26/05/2015	7.8	CVE-2015-3812
bomgar -- remote_support	Bomgar Remote Support before 15.1.1 allows remote attackers to execute arbitrary PHP code via crafted serialized data to unspecified PHP scripts.	25/05/2015	7.5	CVE-2015-0935
h-fj -- mt-phpincgi	mt-phpincgi.php in Hajime Fujimoto mt-phpincgi before 2015-05-15 does not properly restrict URLs, which allows remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via a crafted request, as exploited in the wild in May 2015.	25/05/2015	7.5	CVE-2015-2945
hp -- loadrunner	Buffer overflow in HP LoadRunner 11.52 allows remote attackers to execute arbitrary code via unspecified vectors.	25/05/2015	10.0	CVE-2015-2110
hp -- sitescope	Unspecified vulnerability in HP SiteScope 11.1x before 11.13, 11.2x before 11.24.391, and 11.3x before 11.30.521 allows remote authenticated users to gain privileges via unknown vectors, aka ZDI-CAN-2567.	25/05/2015	8.7	CVE-2015-2120
hp -- network_virtualization	HP Network Virtualization for LoadRunner and Performance Center 8.61 and 11.52 allows remote attackers to read arbitrary files via a crafted filename in a URL to the (1) HttpServlet or (2) NetworkEditorController component, aka ZDI-CAN-2569.	25/05/2015	7.8	CVE-2015-2121
hp -- sdn_van_controller	The REST layer on HP SDN VAN Controller devices 2.5 and earlier allows remote attackers to cause a denial of service via network traffic to the REST port.	25/05/2015	7.8	CVE-2015-2122
hp -- nonstop_safeguard_security	Unspecified vulnerability in HP NonStop Safeguard Security Software H06.x, L15.02, and J06.x before J06.19 allows remote authenticated users to gain privileges by leveraging Expand access.	25/05/2015	9.0	CVE-2015-2123
ibm -- tivoli_storage_manager_fastback	Buffer overflow in the FastBackMount process in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.11.1 has unspecified impact and remote attack vectors.	25/05/2015	7.5	CVE-2015-0120
ibm -- security_siteprotector_system	IBM Security SiteProtector System 3.0 before 3.0.0.7, 3.1 before 3.1.0.4, and 3.1.1 before 3.1.1.2 allows remote authenticated users to execute arbitrary commands with SYSTEM privileges via unspecified vectors.	25/05/2015	9.0	CVE-2015-0160
icu_project -- international_components_for_unicode	The resolveImplicitLevels function in common/ubidi.c in the Unicode Bidirectional Algorithm implementation in ICU4C in International Components for Unicode (ICU) before 55.1 does not properly track directionally isolated pieces of text, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly execute arbitrary code via crafted text.	25/05/2015	7.5	CVE-2014-8146
icu_project -- international_components_for_unicode	The resolveImplicitLevels function in common/ubidi.c in the Unicode Bidirectional Algorithm implementation in ICU4C in International Components for Unicode (ICU) before 55.1 uses an integer data type that is inconsistent with a header file, which allows remote attackers to cause a denial of service (incorrect malloc followed by invalid free) or possibly execute arbitrary code via crafted text.	25/05/2015	7.5	CVE-2014-8147
cisco -- telepresence_tc_software	Cisco TelePresence T, TelePresence TE, and TelePresence TC before 7.1 do not properly implement access control, which allows remote attackers to obtain root privileges by sending packets on the local network and allows physically proximate attackers to obtain root privileges via unspecified vectors, aka Bug ID CSCub67651.	24/05/2015	8.3	CVE-2014-2174
cisco -- telepresence_advanced_media_gateway	The web framework in Cisco TelePresence Advanced Media Gateway Series Software before 1.1(1.40), Cisco TelePresence IP Gateway Series Software, Cisco TelePresence IP VCR Series Software before 3.0(1.27), Cisco TelePresence ISDN Gateway Software before 2.2(1.94), Cisco TelePresence MCU Software before 4.4(3.54) and 4.5 before 4.5(1.45), Cisco TelePresence MSE Supervisor Software before 2.3(1.38), Cisco TelePresence Serial Gateway Series Software before 1.0(1.42), Cisco TelePresence Server Software for Hardware before 3.1(1.98), and Cisco TelePresence Server Software for Virtual Machine before 4.1(1.79) allows remote authenticated users to execute arbitrary commands with root privileges via unspecified vectors, aka Bug IDs CSCul55968, CSCur08993, CSCur15803, CSCur15807, CSCur15825, CSCur15832, CSCur15842, CSCur15850, and CSCur15855.	24/05/2015	9.0	CVE-2015-0713
cisco -- telepresence_tc_software	The network drivers in Cisco TelePresence T, Cisco TelePresence TE, and Cisco TelePresence TC before 7.3.2 allow remote attackers to cause a denial of service (process restart or device reload) via a flood of crafted IP packets, aka Bug ID CSCuj68952.	24/05/2015	7.8	CVE-2015-0722
ibm -- tivoli_storage_manager_fastback	Stack-based buffer overflow in the FastBackMount process in IBM Tivoli Storage Manager FastBack 6.1 before 6.1.11.1 allows remote attackers to execute arbitrary code via unspecified vectors.	24/05/2015	10.0	CVE-2015-1896
ibm -- websphere_portal	IBM WebSphere Portal 8.5 through CF05 allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.	24/05/2015	7.8	CVE-2015-1899

Semana 18/05/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
huawei -- e587_mobile_wifi_firmware	Huawei E587 Mobile WiFi with firmware before 11.203.30.00.00 allows remote attackers to bypass authentication, change configurations, send messages, and cause a denial of service (device restart) via unspecified vectors.	21/05/2015	9.0	CVE-2015-3911
dell -- sonicwall_analyzer	The GMS ViewPoint (GMSVP) web application in Dell Sonicwall GMS, Analyzer, and UMA EM5000 before 7.2 SP4 allows remote authenticated users to execute arbitrary commands via vectors related to configuration.	20/05/2015	9.0	CVE-2015-3990
google -- chrome	common/partial_circular_buffer.cc in Google Chrome before 43.0.2357.65 does not properly handle wraps, which allows remote attackers to bypass a sandbox protection mechanism or cause a denial of service (out-of-bounds write) via vectors that trigger a write operation with a large amount of data, related to the PartialCircularBuffer::Write and PartialCircularBuffer::DoWrite functions.	20/05/2015	7.5	CVE-2015-1252
google -- chrome	core/html/parser/HTMLConstructionSite.cpp in the DOM implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that appends a child to a SCRIPT element, related to the insert and executeReparentTask functions.	20/05/2015	7.5	CVE-2015-1253
google -- chrome	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.	20/05/2015	7.5	CVE-2015-1256
google -- chrome	platform/graphics/filters/FEColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document.	20/05/2015	7.5	CVE-2015-1257
google -- chrome	Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.	20/05/2015	7.5	CVE-2015-1258
google -- chrome	PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	20/05/2015	7.5	CVE-2015-1259
google -- chrome	Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.	20/05/2015	7.5	CVE-2015-1260
google -- chrome	platform/fonts/shaping/HarfBuzzShaper.cpp in Blink, as used in Google Chrome before 43.0.2357.65, does not initialize a certain width field, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Unicode text.	20/05/2015	7.5	CVE-2015-1262
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 43.0.2357.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	20/05/2015	7.5	CVE-2015-1265
google -- chrome	Multiple unspecified vulnerabilities in Google V8 before 4.3.61.21, as used in Google Chrome before 43.0.2357.65, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	20/05/2015	7.5	CVE-2015-3910
ibm -- domino	Stack-based buffer overflow in IBM Domino 8.5 before 8.5.3 FP6 IF7 and 9.0 before 9.0.1 FP3 IF3 allows remote attackers to execute arbitrary code via a crafted BMP image, aka SPR KLYH9TSMLA.	20/05/2015	10.0	CVE-2015-1902
ibm -- domino	Stack-based buffer overflow in IBM Domino 8.5 before 8.5.3 FP6 IF7 and 9.0 before 9.0.1 FP3 IF3 allows remote attackers to execute arbitrary code via a crafted BMP image, aka SPR KLYH9TSN3Y.	20/05/2015	10.0	CVE-2015-1903
kcodes -- netusb	Stack-based buffer overflow in the run_init_sbus function in the KCodes NetUSB module for the Linux kernel, as used in certain NETGEAR products, TP-LINK products, and other products, allows remote attackers to execute arbitrary code by providing a long computer name in a session on TCP port 20005.	20/05/2015	10.0	CVE-2015-3036
oscmax -- oscmax	Multiple SQL injection vulnerabilities in the admin panel in osCMax before 2.5.1 allow (1) remote attackers to execute arbitrary SQL commands via the username parameter in a process action to admin/login.php or (2) remote administrators to execute arbitrary SQL commands via the status parameter to admin/stats_monthly_sales.php or (3) country parameter in a process action to admin/create_account_process.php.	20/05/2015	7.5	CVE-2012-1665
swisscom -- centro_grande_(adb)_dsl_firmware	The certificate verification functions in the HNDS service in Swisscom Centro Grande (ADB) DSL routers with firmware before 6.14.00 allows remote attackers to access the management functions via unknown vectors.	20/05/2015	10.0	CVE-2015-1188
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 6.1 through 6.1.0.47, 7.0 before 7.0.0.39, 8.0 before 8.0.0.11, and 8.5 before 8.5.5.6 allows remote attackers to execute arbitrary code by sending crafted instructions in a management-port session.	19/05/2015	10.0	CVE-2015-1920
module-signature_project -- module-signature	Module::Signature before 0.74 allows remote attackers to execute arbitrary shell commands via a crafted SIGNATURE file which is not properly handled when generating checksums from a signed manifest.	19/05/2015	10.0	CVE-2015-3408
module-signature_project -- module-signature	Untrusted search path vulnerability in Module::Signature before 0.75 allows local users to gain privileges via a Trojan horse module under the current working directory, as demonstrated by a Trojan horse Text::Diff module.	19/05/2015	7.2	CVE-2015-3409
unzoo -- unzoo	Buffer overflow in the EntrReadArch function in unzoo might allow remote attackers to execute arbitrary code via unspecified vectors.	19/05/2015	10.0	CVE-2015-1845
unzoo -- unzoo	unzoo allows remote attackers to cause a denial of service (infinite loop and resource consumption) via unspecified vectors to the (1) ExtrArch or (2) ListArch function, related to pointer handling.	19/05/2015	7.8	CVE-2015-1846
docker -- docker	Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.	18/05/2015	7.2	CVE-2015-3627
docker -- libcontainer	Libcontainer 1.6.0, as used in Docker Engine, allows local users to escape containerization ("mount namespace breakout") and write to arbitrary file on the host system via a symlink attack in an image when respawning a container.	18/05/2015	7.2	CVE-2015-3629
docker -- docker	Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.	18/05/2015	7.2	CVE-2015-3630
gns3 -- gns3	Untrusted search path vulnerability in GNS3 before 1.2.3 allows local users to gain privileges via a Trojan horse uuid.dll in an unspecified directory.	18/05/2015	7.2	CVE-2015-2667
infocus -- in3128hd_firmware	The InFocus IN3128HD projector with firmware 0.26 allows remote attackers to bypass authentication via a direct request to main.html.	18/05/2015	10.0	CVE-2014-8383
infocus -- in3128hd_firmware	The InFocus IN3128HD projector with firmware 0.26 does not restrict access to cgi-bin/webctrl.cgi.elf, which allows remote attackers to modify the DHCP server and device IP configuration, reboot the device, change the device name, and have other unspecified impact via a crafted request.	18/05/2015	9.4	CVE-2014-8384
libuv_project -- libuv	libuv before 0.10.34 does not properly drop group privileges, which allows context-dependent attackers to gain privileges via unspecified vectors.	18/05/2015	10.0	CVE-2015-0278
powerdns -- authoritative	The label decompression functionality in PowerDNS Recursor 3.5.x, 3.6.x before 3.6.3, and 3.7.x before 3.7.2 and Authoritative (Auth) Server 3.2.x, 3.3.x before 3.3.2, and 3.4.x before 3.4.4 allows remote attackers to cause a denial of service (CPU consumption or crash) via a request with a name that refers to itself.	18/05/2015	7.8	CVE-2015-1868
proftpd -- proftpd	The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.	18/05/2015	10.0	CVE-2015-3306
cisco -- unified_communications_manager	Cisco Unified Communications Manager 10.0(1.10000.12) allows local users to gain privileges via a command string in an unspecified parameter, aka Bug ID CSCut19546.	16/05/2015	7.2	CVE-2015-0717
hancom -- hanword_viewer_2007	Integer overflow in the HwpApp::CHncSDS_Manager function in Hancom Office HanWord processor, as used in Hwp 2014 VP before 9.1.0.2342, HanWord Viewer 2007 and Viewer 2010 8.5.6.1158, and HwpViewer 2014 VP 9.1.0.2186, allows remote attackers to cause a denial of service (crash) and possibly "influence the program's execution flow" via a document with a large paragraph size, which triggers heap corruption.	15/05/2015	7.5	CVE-2015-2810
wpsymposium -- wp_symposium	SQL injection vulnerability in forum.php in the WP Symposium plugin before 15.4 for WordPress allows remote attackers to execute arbitrary SQL commands via the show parameter in the QUERY_STRING to the default URI.	15/05/2015	7.5	CVE-2015-3325

Semana 11/05/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
clip-bucket -- clipbucket	Multiple SQL injection vulnerabilities in ClipBucket 2.6 Revision 738 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) uid parameter in an add_friend action to ajax.php; id parameter in a (2) share_object, (3) add_to_fav, (4) rating, or (5) flag_object action to ajax.php; cid parameter in an (6) add_new_item, (7) remove_collection_item, (8) get_item, or (9) load_more_items action to ajax.php; (10) ci_id parameter in a get_item action to ajax.php; user parameter to (11) user_contacts.php or (12) view_channel.php; (13) pid parameter to view_page.php; (14) tid parameter to view_topic.php; or (15) v parameter to watch_video.php.	14/05/2015	7.5	CVE-2012-5849
mcafee -- epo_deep_command	Multiple unquoted Windows search path vulnerabilities in the (1) Client Management and (2) Gateway in McAfee ePO Deep Command 2.1 and 2.2 before HF 1058831 allow local users to gain privileges via unspecified vectors.	14/05/2015	7.2	CVE-2015-3987
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	14/05/2015	7.5	CVE-2015-2708
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 38.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	14/05/2015	7.5	CVE-2015-2709
mozilla -- firefox	The asm.js implementation in Mozilla Firefox before 38.0 does not properly determine heap lengths during identification of cases in which bounds checking may be safely skipped, which allows remote attackers to trigger out-of-bounds write operations and possibly execute arbitrary code, or trigger out-of-bounds read operations and possibly obtain sensitive information from process memory, via crafted JavaScript.	14/05/2015	7.5	CVE-2015-2712
mozilla -- firefox	Buffer overflow in the XML parser in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allows remote attackers to execute arbitrary code by providing a large amount of compressed XML data.	14/05/2015	7.5	CVE-2015-2716
quassel-irc -- quassel	Quassel before 0.12.2 does not properly re-initialize the database session when the PostgreSQL database is restarted, which allows remote attackers to conduct SQL injection attacks via a \ (backslash) in a message. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4422.	14/05/2015	7.5	CVE-2015-3427
redhat -- network_satellite	XML external entity (XXE) in the RPC interface in Spacewalk and Red Hat Network (RHN) Satellite 5.7 and earlier allows remote attackers to read arbitrary files and possibly have other unspecified impact via unknown vectors.	14/05/2015	7.5	CVE-2014-8162
adobe -- acrobat	Multiple heap-based buffer overflows in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to execute arbitrary code via unknown vectors.	13/05/2015	10.0	CVE-2014-9160
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3046
adobe -- acrobat	Buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unknown vectors.	13/05/2015	10.0	CVE-2015-3048
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3049
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3050
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3051
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3056, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3052
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3054, CVE-2015-3055, CVE-2015-3059, and CVE-2015-3075.	13/05/2015	10.0	CVE-2015-3053
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3055, CVE-2015-3059, and CVE-2015-3075.	13/05/2015	10.0	CVE-2015-3054
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3059, and CVE-2015-3075.	13/05/2015	7.5	CVE-2015-3055
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3057, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3056
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3070, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3057
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, and CVE-2015-3075.	13/05/2015	10.0	CVE-2015-3059
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3060
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3061
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3062
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3063
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3064
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3065
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3066
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3067
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3068
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3071, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3069
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, and CVE-2015-3076.	13/05/2015	10.0	CVE-2015-3070

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3072, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3071
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3073, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3072
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, and CVE-2015-3074.	13/05/2015	10.0	CVE-2015-3073
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allow attackers to bypass intended restrictions on JavaScript API execution via unspecified vectors, a different vulnerability than CVE-2015-3060, CVE-2015-3061, CVE-2015-3062, CVE-2015-3063, CVE-2015-3064, CVE-2015-3065, CVE-2015-3066, CVE-2015-3067, CVE-2015-3068, CVE-2015-3069, CVE-2015-3071, CVE-2015-3072, and CVE-2015-3073.	13/05/2015	10.0	CVE-2015-3074
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, and CVE-2015-3059.	13/05/2015	10.0	CVE-2015-3075
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 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-2014-9161, CVE-2015-3046, CVE-2015-3049, CVE-2015-3050, CVE-2015-3051, CVE-2015-3052, CVE-2015-3056, CVE-2015-3057, and CVE-2015-3070.	13/05/2015	10.0	CVE-2015-3076
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3084 and CVE-2015-3086.	13/05/2015	10.0	CVE-2015-3077
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3089, CVE-2015-3090, and CVE-2015-3093.	13/05/2015	10.0	CVE-2015-3078
adobe -- adobe_air	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.	13/05/2015	10.0	CVE-2015-3080
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3077 and CVE-2015-3086.	13/05/2015	10.0	CVE-2015-3084
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3077 and CVE-2015-3084.	13/05/2015	10.0	CVE-2015-3086
adobe -- adobe_air	Integer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.	13/05/2015	10.0	CVE-2015-3087
adobe -- adobe_air	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.	13/05/2015	10.0	CVE-2015-3088
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3090, and CVE-2015-3093.	13/05/2015	10.0	CVE-2015-3089
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3089, and CVE-2015-3093.	13/05/2015	10.0	CVE-2015-3090
adobe -- adobe_air	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3089, and CVE-2015-3090.	13/05/2015	10.0	CVE-2015-3093
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1706, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.	13/05/2015	9.3	CVE-2015-1658
microsoft -- .net_framework	The Windows DirectWrite library, as used in Microsoft .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2; Office 2007 SP3 and 2010 SP2; Live Meeting 2007 Console; Lync 2010; Lync 2010 Attendee; Lync 2013 SP1; Lync Basic 2013 SP1; Silverlight 5 before 5.1.40416.00; and Silverlight 5 Developer Runtime before 5.1.40416.00, allows remote attackers to execute arbitrary code via a crafted TrueType font, aka "TrueType Font Parsing Vulnerability."	13/05/2015	9.3	CVE-2015-1671
microsoft -- .net_framework	The Windows Forms (aka WinForms) libraries in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2 allow user-assisted remote attackers to execute arbitrary code via a crafted partial-trust application, aka "Windows Forms Elevation of Privilege Vulnerability."	13/05/2015	9.3	CVE-2015-1673
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699.	13/05/2015	9.3	CVE-2015-1675
microsoft -- excel	Microsoft Office 2010 SP2, Excel 2010 SP2, PowerPoint 2010 SP2, Word 2010 SP2, Office 2013 SP1, Excel 2013 SP1, PowerPoint 2013 SP1, Word 2013 SP1, Office 2013 RT SP1, Excel 2013 RT SP1, PowerPoint 2013 RT SP1, Word 2013 RT SP1, Office for Mac 2011, Excel for Mac 2011, PowerPoint for Mac 2011, Word for Mac 2011, PowerPoint Viewer, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, Excel Services on SharePoint Server 2010 SP2 and 2013 SP1, Office Web Apps 2010 SP2, Excel Web App 2010 SP2, Office Web Apps Server 2013 SP1, SharePoint Foundation 2010 SP2, and SharePoint Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	13/05/2015	9.3	CVE-2015-1682
microsoft -- office	Microsoft Office 2007 SP3 allows remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability."	13/05/2015	9.3	CVE-2015-1683
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1705.	13/05/2015	9.3	CVE-2015-1689
microsoft -- internet_explorer	Microsoft Internet Explorer 8 and 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1712.	13/05/2015	9.3	CVE-2015-1691
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1710.	13/05/2015	9.3	CVE-2015-1694
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1675, CVE-2015-1696, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699.	13/05/2015	9.3	CVE-2015-1695
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1697, CVE-2015-1698, and CVE-2015-1699.	13/05/2015	9.3	CVE-2015-1696
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1698, and CVE-2015-1699.	13/05/2015	9.3	CVE-2015-1697
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1699.	13/05/2015	9.3	CVE-2015-1698

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_7	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, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted Journal file, aka "Windows Journal Remote Code Execution Vulnerability," a different vulnerability than CVE-2015-1675, CVE-2015-1695, CVE-2015-1696, CVE-2015-1697, and CVE-2015-1698.	13/05/2015	9.3	CVE-2015-1699
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1689.	13/05/2015	9.3	CVE-2015-1705
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1711, CVE-2015-1717, and CVE-2015-1718.	13/05/2015	9.3	CVE-2015-1706
microsoft -- internet_explorer	Microsoft Internet Explorer 7 and 8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	13/05/2015	9.3	CVE-2015-1708
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."	13/05/2015	9.3	CVE-2015-1709
microsoft -- internet_explorer	Microsoft Internet Explorer 6 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-2015-1694.	13/05/2015	9.3	CVE-2015-1710
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1717, and CVE-2015-1718.	13/05/2015	9.3	CVE-2015-1711
microsoft -- internet_explorer	Microsoft Internet Explorer 8 and 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1691.	13/05/2015	9.3	CVE-2015-1712
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."	13/05/2015	9.3	CVE-2015-1714
microsoft -- silverlight	Microsoft Silverlight 5 before 5.1.40416.00 allows remote attackers to bypass intended integrity-level restrictions via a crafted Silverlight application, aka "Microsoft Silverlight Out of Browser Application Vulnerability."	13/05/2015	9.3	CVE-2015-1715
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1718.	13/05/2015	9.3	CVE-2015-1717
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1658, CVE-2015-1706, CVE-2015-1711, and CVE-2015-1717.	13/05/2015	9.3	CVE-2015-1718
qemu -- qemu	The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands, aka VENOM.	13/05/2015	7.7	CVE-2015-3456
citrix -- netscaler_application_delivery_controller_firmware	Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway before 10.5 Build 53.9 through 55.8 and 10.5.e Build 53-9010.e allow remote attackers to cause a denial of service (reboot) via unspecified vectors.	12/05/2015	7.8	CVE-2015-2829
goautodial -- goadmin_ce	Unrestricted file upload vulnerability in go_audiostore.php in the audiostore (Voice Files) upload functionality in GoAutoDial GoAdmin CE 3.x before 3.3-1421902800 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in sounds/.	12/05/2015	10.0	CVE-2015-2842
goautodial -- goadmin_ce	Multiple SQL injection vulnerabilities in GoAutoDial GoAdmin CE before 3.3-1421902800 allow remote attackers to execute arbitrary SQL commands via the (1) user_name or (2) user_pass parameter in go_login.php or the PATH_INFO to (3) go_login/validate_credentials/admin/ or (4) index.php/go_site/go_get_user_info/.	12/05/2015	7.5	CVE-2015-2843
goautodial -- goadmin_ce	The cpanel function in go_site.php in GoAutoDial GoAdmin CE before 3.3-1420434000 allows remote attackers to execute arbitrary commands via the $action portion of the PATH_INFO.	12/05/2015	10.0	CVE-2015-2844
goautodial -- goadmin_ce	The cpanel function in go_site.php in GoAutoDial GoAdmin CE before 3.3-1421902800 allows remote attackers to execute arbitrary commands via the $type portion of the PATH_INFO.	12/05/2015	10.0	CVE-2015-2845
lenovo -- system_update	Lenovo System Update (formerly ThinkVantage System Update) before 5.06.0034 uses predictable security tokens, which allows local users to gain privileges by sending a valid token with a command to the System Update service (SUService.exe) through an unspecified named pipe.	12/05/2015	7.2	CVE-2015-2219
lenovo -- system_update	Lenovo System Update (formerly ThinkVantage System Update) before 5.06.0034 does not properly validate CA chains during signature validation, which allows man-in-the-middle attackers to upload and execute arbitrary files via a crafted certificate.	12/05/2015	8.3	CVE-2015-2233
sap -- customer_relationship_management	Unspecified vulnerability in the Business Rules Framework (CRM-BF-BRF) in SAP CRM allows attackers to execute arbitrary code via unknown vectors, aka SAP Security Note 2097534.	12/05/2015	7.5	CVE-2015-3979
sap -- customer_relationship_management	SQL injection vulnerability in the Business Rules Framework (CRM-BF-BRF) in SAP CRM allows attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2097534.	12/05/2015	7.5	CVE-2015-3980

Semana 04/05/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- unified_computing_system_central_software	Cisco UCS Central Software 1.2 and earlier allows remote attackers to execute arbitrary commands via a crafted HTTP request, aka Bug ID CSCut46961.	06/05/2015	10.0	CVE-2015-0701
emc -- autostart	ftagent.exe in EMC AutoStart 5.4.x and 5.5.x before 5.5.0.508 HF4 allows remote attackers to execute arbitrary commands via crafted packets.	06/05/2015	9.3	CVE-2015-0538
alienvault -- unified_security_management	The Framework Daemon in AlienVault Unified Security Management before 4.15 allows remote attackers to execute arbitrary Python code via a crafted plugin configuration file (.cfg).	01/05/2015	9.3	CVE-2015-3446
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.135 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	01/05/2015	7.5	CVE-2015-1250
realtek -- realtek_sdk	The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code via a crafted NewInternalClient request.	01/05/2015	10.0	CVE-2014-8361
samsung -- samsung_security_manager	Samsung Security Manager (SSM) before 1.31 allows remote attackers to execute arbitrary code by uploading a file with an HTTP (1) PUT or (2) MOVE request.	01/05/2015	10.0	CVE-2015-3435