Histórico de vulnerabilidades de Diciembre del 2015

Semana 28/12/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ampedwireless -- r10000_firmware	The web administration interface on Amped Wireless R10000 devices with firmware 2.5.2.11 has a default password of admin for the admin account, which allows remote attackers to obtain administrative privileges by leveraging a LAN session.	31/12/2015	9.3	CVE-2015-7277
belkin -- n600_db_wi-fi_dual-band_n\+_router_f9k1102_firmware	The web management interface on Belkin F9K1102 2 devices with firmware 2.10.17 has a blank password, which allows remote attackers to obtain administrative privileges by leveraging a LAN session.	31/12/2015	9.3	CVE-2015-5988
belkin -- n600_db_wi-fi_dual-band_n\+_router_f9k1102_firmware	Belkin F9K1102 2 devices with firmware 2.10.17 rely on client-side JavaScript code for authorization, which allows remote attackers to obtain administrative privileges via certain changes to LockStatus and Login_Success values.	31/12/2015	10.0	CVE-2015-5989
idera -- uptime_infrastructure_monitor	Buffer overflow in the up.time client in Idera Uptime Infrastructure Monitor 7.4 might allow remote attackers to execute arbitrary code via long command input.	31/12/2015	7.5	CVE-2015-2895
mediabridge -- medialink_mwn-wapr300n_firmware	The web management interface on Mediabridge Medialink MWN-WAPR300N devices with firmware 5.07.50 has a default password of admin for the admin account and a default password of password for the medialink account, which allows remote attackers to obtain administrative privileges by leveraging a Wi-Fi session.	31/12/2015	7.9	CVE-2015-5994
readynet_solutions -- wrt300n-dd_firmware	The web administration interface on ReadyNet WRT300N-DD devices with firmware 1.0.26 has a default password of admin for the admin account, which allows remote attackers to obtain administrative privileges by leveraging a LAN session.	31/12/2015	10.0	CVE-2015-7280
seagate -- goflex_sattelite	Seagate GoFlex Satellite, Seagate Wireless Mobile Storage, Seagate Wireless Plus Mobile Storage, and LaCie FUEL devices with firmware before 3.4.1.105 have a default password of root for the root account, which allows remote attackers to obtain administrative access via a TELNET session.	31/12/2015	10.0	CVE-2015-2874
seagate -- goflex_sattelite	Absolute path traversal vulnerability on Seagate GoFlex Satellite, Seagate Wireless Mobile Storage, Seagate Wireless Plus Mobile Storage, and LaCie FUEL devices with firmware before 3.4.1.105 allows remote attackers to read arbitrary files via a full pathname in a download request during a Wi-Fi session.	31/12/2015	7.8	CVE-2015-2875
seagate -- goflex_sattelite	Unrestricted file upload vulnerability on Seagate GoFlex Satellite, Seagate Wireless Mobile Storage, Seagate Wireless Plus Mobile Storage, and LaCie FUEL devices with firmware before 3.4.1.105 allows remote attackers to execute arbitrary code by uploading a file to /media/sda2 during a Wi-Fi session.	31/12/2015	8.3	CVE-2015-2876
tenda -- n3_wireless_n150	Mediabridge Medialink MWN-WAPR300N devices with firmware 5.07.50 and Tenda N3 Wireless N150 devices allow remote attackers to obtain administrative access via a certain admin substring in an HTTP Cookie header.	31/12/2015	10.0	CVE-2015-5995
zyxel -- nbg-418n	ZyXEL P-660HW-T1 2 devices with ZyNOS firmware 3.40(AXH.0), PMG5318-B20A devices with firmware 1.00AANC0b5, and NBG-418N devices have a default password of 1234 for the admin account, which allows remote attackers to obtain administrative access via unspecified vectors.	31/12/2015	10.0	CVE-2015-6016
zyxel -- pmg5318-b20a_firmware	The diagnostic-ping implementation on ZyXEL PMG5318-B20A devices with firmware before 1.00(AANC.2)C0 allows remote attackers to execute arbitrary commands via the PingIPAddr parameter.	31/12/2015	10.0	CVE-2015-6018
zyxel -- pmg5318-b20a_firmware	ZyXEL PMG5318-B20A devices with firmware 1.00AANC0b5 allow remote authenticated users to obtain administrative privileges by leveraging access to the user account.	31/12/2015	8.3	CVE-2015-6020
zyxel -- nbg-418n_firmware	The web administration interface on ZyXEL NBG-418N devices with firmware 1.00(AADZ.3)C0 has a default password of 1234 for the admin account, which allows remote attackers to obtain administrative privileges by leveraging a LAN session.	31/12/2015	9.3	CVE-2015-7283
corega -- cg-wlbargs_firmware	Corega CG-WLBARGS devices allow remote attackers to perform administrative operations via unspecified vectors.	30/12/2015	10.0	CVE-2015-7792
zte -- zxhn_h108n_r1a_firmware	Absolute path traversal vulnerability in cgi-bin/webproc on ZTE ZXHN H108N R1A devices before ZTE.bhs.ZXHNH108NR1A.k_PE allows remote attackers to read arbitrary files via a full pathname in the getpage parameter.	30/12/2015	7.8	CVE-2015-7250
zte -- zxhn_h108n_r1a_firmware	ZTE ZXHN H108N R1A devices before ZTE.bhs.ZXHNH108NR1A.k_PE have a hardcoded password of root for the root account, which allows remote attackers to obtain administrative access via a TELNET session.	30/12/2015	10.0	CVE-2015-7251
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8460, CVE-2015-8636, and CVE-2015-8645.	28/12/2015	10.0	CVE-2015-8459
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8636, and CVE-2015-8645.	28/12/2015	9.3	CVE-2015-8460
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8634
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8635
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8645.	28/12/2015	9.3	CVE-2015-8636
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8638
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8639
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8640
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8641
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8642
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8643
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."	28/12/2015	9.3	CVE-2015-8644
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8636.	28/12/2015	9.3	CVE-2015-8645
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8646
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8647
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8649, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8648
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8650.	28/12/2015	9.3	CVE-2015-8649
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.	28/12/2015	9.3	CVE-2015-8650
adobe -- air	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.	28/12/2015	9.3	CVE-2015-8651
emc -- vplex_geosynchrony	EMC VPLEX GeoSynchrony 5.4 SP1 before P3 and 5.5 before Patch 1 has a default password for the root account, which allows local users to gain privileges by leveraging a login session.	28/12/2015	7.2	CVE-2015-6850
linux -- linux_kernel	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.	28/12/2015	7.2	CVE-2015-8660
ephiphanyheathdata -- cardio_server	The login page in Epiphany Cardio Server 3.3, 4.0, and 4.1 mishandles authentication requests, which allows remote attackers to conduct LDAP injection attacks, and consequently bypass intended access restrictions, via a crafted URL.	27/12/2015	7.5	CVE-2015-6538
epiphanyhealthdata -- cardio_server	SQL injection vulnerability in the login page in Epiphany Cardio Server 3.3 allows remote attackers to execute arbitrary SQL commands via a crafted URL.	27/12/2015	7.5	CVE-2015-6537

Semana 21/12/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8460, CVE-2015-8636, and CVE-2015-8645.	28/12/2015	10.0	CVE-2015-8459
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.	28/12/2015	9.3	CVE-2015-8650
emc -- vplex_geosynchrony	EMC VPLEX GeoSynchrony 5.4 SP1 before P3 and 5,5 before Patch 1 has a default password for the root account, which allows local users to gain privileges by leveraging a login session.	28/12/2015	7.2	CVE-2015-6850
linux -- linux_kernel	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.	28/12/2015	7.2	CVE-2015-8660
ephiphanyheathdata -- cardio_server	The login page in Epiphany Cardio Server 3.3, 4.0, and 4.1 mishandles authentication requests, which allows remote attackers to conduct LDAP injection attacks, and consequently bypass intended access restrictions, via a crafted URL.	27/12/2015	7.5	CVE-2015-6538
epiphanyhealthdata -- cardio_server	SQL injection vulnerability in the login page in Epiphany Cardio Server 3.3 allows remote attackers to execute arbitrary SQL commands via a crafted URL.	27/12/2015	7.5	CVE-2015-6537
adcon -- a840_telemetry_gateway_base_station_firmware	Adcon Telemetry A840 Telemetry Gateway Base Station has hardcoded credentials, which allows remote attackers to obtain administrative access via unspecified vectors.	23/12/2015	10.0	CVE-2015-7930
dovestones -- ad_self_password_reset	The PasswordReset.Controllers.ResetController.ChangePasswordIndex method in PasswordReset.dll in Dovestones AD Self Password Reset before 3.0.4.0 allows remote attackers to reset arbitrary passwords via a crafted request with a valid username.	23/12/2015	7.5	CVE-2015-8267
ewon -- ewon_firmware	eWON devices with firmware before 10.1s0 do not trigger the discarding of browser session data in response to a log-off action, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.	23/12/2015	7.5	CVE-2015-7924
ffmpeg -- ffmpeg	The h264_slice_header_init function in libavcodec/h264_slice.c in FFmpeg before 2.8.3 does not validate the relationship between the number of threads and the number of slices, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted H.264 data.	23/12/2015	7.5	CVE-2015-8661
ffmpeg -- ffmpeg	The ff_dwt_decode function in libavcodec/jpeg2000dwt.c in FFmpeg before 2.8.4 does not validate the number of decomposition levels before proceeding with Discrete Wavelet Transform decoding, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data.	23/12/2015	7.5	CVE-2015-8662
ffmpeg -- ffmpeg	The ff_get_buffer function in libavcodec/utils.c in FFmpeg before 2.8.4 preserves width and height values after a failure, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted .mov file.	23/12/2015	7.5	CVE-2015-8663
google -- chrome	The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.	23/12/2015	10.0	CVE-2015-6792
google -- chrome	Integer overflow in the WebCursor::Deserialize function in content/common/cursors/webcursor.cc in Google Chrome before 47.0.2526.106 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an RGBA pixel array with crafted dimensions, a different vulnerability than CVE-2015-6792.	23/12/2015	7.5	CVE-2015-8664
isc -- kea	The kea-dhcp4 and kea-dhcp6 servers 0.9.2 and 1.0.0-beta in ISC Kea, when certain debugging settings are used, allow remote attackers to cause a denial of service (daemon crash) via a malformed packet.	22/12/2015	7.1	CVE-2015-8373
rsa -- securid_web_agent	EMC RSA SecurID Web Agent before 8.0 allows physically proximate attackers to bypass the privacy-screen protection mechanism by leveraging an unattended workstation and running DOM Inspector.	22/12/2015	7.2	CVE-2015-6851
saia_burgess_controls -- pcd1.m0xx0_firmware	Saia Burgess PCD1.M0xx0, PCD1.M2xx0, PCD2.M5xx0, PCD3.Mxx60, PCD3.Mxxx0, PCD7.D4xxD, PCD7.D4xxV, PCD7.D4xxWTPF, and PCD7.D4xxxT5F devices before 1.24.50 and PCD3.T665 and PCD3.T666 devices before 1.24.41 have hardcoded credentials, which allows remote attackers to obtain administrative access via an FTP session.	22/12/2015	10.0	CVE-2015-7911
apache -- hbase	Apache HBase 0.98 before 0.98.12.1, 1.0 before 1.0.1.1, and 1.1 before 1.1.0.1, as used in IBM InfoSphere BigInsights 3.0, 3.0.0.1, and 3.0.0.2 and other products, uses incorrect ACLs for ZooKeeper coordination state, which allows remote attackers to cause a denial of service (daemon outage), obtain sensitive information, or modify data via unspecified client traffic.	21/12/2015	7.5	CVE-2015-1836
emc -- isilon_onefs	EMC Isilon OneFS 7.1 before 7.1.1.8, 7.2.0 before 7.2.0.4, and 7.2.1 before 7.2.1.1 allows remote authenticated administrators to bypass a SmartLock root-login restriction by creating a root account and establishing a login session.	21/12/2015	9.0	CVE-2015-4545
honeywell -- midas_black_firmware	Honeywell Midas gas detectors before 1.13b3 and Midas Black gas detectors before 2.13b3 allow remote attackers to discover cleartext passwords by sniffing the network.	21/12/2015	9.3	CVE-2015-7908
loytec -- l-switch_and_l-ip_firmware	LOYTEC LIP-3ECTB 6.0.1, LINX-100, LVIS-3E100, and LIP-ME201 devices allow remote attackers to read a password-hash backup file via unspecified vectors.	21/12/2015	10.0	CVE-2015-7906
moxa -- oncell_central_manager	The MessageBrokerServlet servlet in Moxa OnCell Central Manager before 2.2 does not require authentication, which allows remote attackers to obtain administrative access via a command, as demonstrated by the addUserAndGroup action.	21/12/2015	7.5	CVE-2015-6480
moxa -- oncell_central_manager	The login function in the RequestController class in Moxa OnCell Central Manager before 2.2 has a hardcoded root password, which allows remote attackers to obtain administrative access via a login session.	21/12/2015	7.5	CVE-2015-6481
schneider-electric -- bmxnoc0401	Stack-based buffer overflow in the GoAhead Web Server on Schneider Electric Modicon M340 PLC BMXNOx and BMXPx devices allows remote attackers to execute arbitrary code via a long password in HTTP Basic Authentication data.	21/12/2015	10.0	CVE-2015-7937
vmware -- vcenter_orchestrator	Serialized-object interfaces in VMware vRealize Orchestrator 6.x, vCenter Orchestrator 5.x, vRealize Operations 6.x, vCenter Operations 5.x, and vCenter Application Discovery Manager (vADM) 7.x allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections library.	20/12/2015	7.5	CVE-2015-6934
juniper -- screenos	Juniper ScreenOS 6.2.0r15 through 6.2.0r18, 6.3.0r12 before 6.3.0r12b, 6.3.0r13 before 6.3.0r13b, 6.3.0r14 before 6.3.0r14b, 6.3.0r15 before 6.3.0r15b, 6.3.0r16 before 6.3.0r16b, 6.3.0r17 before 6.3.0r17b, 6.3.0r18 before 6.3.0r18b, 6.3.0r19 before 6.3.0r19b, and 6.3.0r20 before 6.3.0r21 allows remote attackers to obtain administrative access by entering an unspecified password during a (1) SSH or (2) TELNET session.	19/12/2015	10.0	CVE-2015-7755

Semana 14/12/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_policy_infrastructure_controller	The boot manager in Cisco Application Policy Infrastructure Controller (APIC) 1.1(0.920a) allows local users to bypass intended access restrictions and obtain single-user-mode root access via unspecified vectors, aka Bug ID CSCuu83985.	18/12/2015	7.2	CVE-2015-6424
cisco -- prime_network_services_controller	Cisco Prime Network Services Controller 3.0 allows local users to bypass intended access restrictions and execute arbitrary commands via additional parameters to an unspecified command, aka Bug ID CSCus99427.	18/12/2015	7.2	CVE-2015-6426
accunetix -- web_vulnerability_scanner	The AcuWVSSchedulerv10 service in Acunetix Web Vulnerability Scanner (WVS) before 10 build 20151125 allows local users to gain privileges via a command parameter in the reporttemplate property in a params JSON object to api/addScan.	17/12/2015	7.2	CVE-2015-4027
cacti -- cacti	SQL injection vulnerability in include/top_graph_header.php in Cacti 0.8.8f and earlier allows remote attackers to execute arbitrary SQL commands via the rra_id parameter in a properties action to graph.php.	17/12/2015	7.5	CVE-2015-8369
cool_video_gallery_project -- cool_video_gallery	lib/core.php in the Cool Video Gallery plugin 1.9 for WordPress allows remote attackers to execute arbitrary code via shell metacharacters in the "Width of preview image" and possibly other input fields in the "Video Gallery Settings" page.	17/12/2015	7.5	CVE-2015-7527
gnu -- glibc	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.	17/12/2015	7.2	CVE-2015-5277
linuxfoundation -- cups-filters	Incomplete blacklist vulnerability in util.c in foomatic-rip in cups-filters 1.0.42 before 1.2.0 and in foomatic-filters in Foomatic 4.0.x allows remote attackers to execute arbitrary commands via ` (backtick) characters in a print job.	17/12/2015	7.5	CVE-2015-8327
sap -- mobile_platform	The SysAdminWebTool servlets in SAP Mobile Platform allow remote attackers to bypass authentication and obtain sensitive information, gain privileges, or have unspecified other impact via unknown vectors, aka SAP Security Note 2227855.	17/12/2015	7.5	CVE-2015-8600
xen -- xen	Xen 4.6.x and earlier does not properly enforce limits on page order inputs for the (1) XENMEM_increase_reservation, (2) XENMEM_populate_physmap, (3) XENMEM_exchange, and possibly other HYPERVISOR_memory_op suboperations, which allows ARM guest OS administrators to cause a denial of service (CPU consumption, guest reboot, or watchdog timeout and host reboot) and possibly have unspecified other impact via unknown vectors.	17/12/2015	7.2	CVE-2015-8338
xen -- xen	The libxl toolstack library in Xen 4.1.x through 4.6.x does not properly release mappings of files used as kernels and initial ramdisks when managing multiple domains in the same process, which allows attackers to cause a denial of service (memory and disk consumption) by starting domains.	17/12/2015	7.8	CVE-2015-8341
apache -- tomee	The EjbObjectInputStream class in Apache TomEE allows remote attackers to execute arbitrary commands via a serialized Java stream.	16/12/2015	7.5	CVE-2015-8581
bitrix -- mpbuilder	Directory traversal vulnerability in the bitrix.mpbuilder module before 1.0.12 for Bitrix allows remote administrators to include and execute arbitrary local files via a .. (dot dot) in the element name of the "work" array parameter to admin/bitrix.mpbuilder_step2.php.	16/12/2015	9.0	CVE-2015-8358
isc -- bind	Race condition in resolver.c in named in ISC BIND 9.9.8 before 9.9.8-P2 and 9.10.3 before 9.10.3-P2 allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via unspecified vectors.	16/12/2015	7.1	CVE-2015-8461
joomla -- joomla!	Joomla! 1.5.x, 2.x, and 3.x before 3.4.6 allow remote attackers to conduct PHP object injection attacks and execute arbitrary PHP code via the HTTP User-Agent header, as exploited in the wild in December 2015.	16/12/2015	7.5	CVE-2015-8562
joomla -- joomla!	Directory traversal vulnerability in Joomla! 3.4.x before 3.4.6 allows remote attackers to have unspecified impact via directory traversal sequences in the XML install file in an extension package archive.	16/12/2015	7.5	CVE-2015-8564
joomla -- joomla!	Directory traversal vulnerability in Joomla! 3.2.0 through 3.3.x and 3.4.x before 3.4.6 allows remote attackers to have unspecified impact via unknown vectors.	16/12/2015	7.5	CVE-2015-8565
joomla -- session	The Session package 1.x before 1.3.1 for Joomla! Framework allows remote attackers to execute arbitrary code via unspecified session values.	16/12/2015	7.5	CVE-2015-8566
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	16/12/2015	10.0	CVE-2015-7201
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 43.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	16/12/2015	10.0	CVE-2015-7202
mozilla -- firefox	Buffer overflow in the DirectWriteFontInfo::LoadFontFamilyData function in gfx/thebes/gfxDWriteFontList.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font-family name.	16/12/2015	10.0	CVE-2015-7203
mozilla -- firefox	Integer underflow in the RTPReceiverVideo::ParseRtpPacket function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 might allow remote attackers to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a crafted WebRTC RTP packet.	16/12/2015	10.0	CVE-2015-7205
mozilla -- firefox	Use-after-free vulnerability in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code by triggering attempted use of a data channel that has been closed by a WebRTC function.	16/12/2015	7.5	CVE-2015-7210
mozilla -- firefox	Integer overflow in the mozilla::layers::BufferTextureClient::AllocateForSurface function in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.5 allows remote attackers to execute arbitrary code by triggering a graphics operation that requires a large texture allocation.	16/12/2015	7.5	CVE-2015-7212
mozilla -- firefox	Buffer overflow in the XDRBuffer::grow function in js/src/vm/Xdr.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.	16/12/2015	10.0	CVE-2015-7220
mozilla -- firefox	Buffer overflow in the nsDeque::GrowCapacity function in xpcom/glue/nsDeque.cpp in Mozilla Firefox before 43.0 might allow remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a deque size change.	16/12/2015	10.0	CVE-2015-7221
apache -- commons_collections	Serialized-object interfaces in certain Cisco Collaboration and Social Media; Endpoint Clients and Client Software; Network Application, Service, and Acceleration; Network and Content Security Devices; Network Management and Provisioning; Routing and Switching - Enterprise and Service Provider; Unified Computing; Voice and Unified Communications Devices; Video, Streaming, TelePresence, and Transcoding Devices; Wireless; and Cisco Hosted Services products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	15/12/2015	7.5	CVE-2015-6420

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- spa300_firmware	The TFTP implementation on Cisco Small Business SPA30x, SPA50x, SPA51x phones 7.5.7 improperly validates firmware-image file integrity, which allows local users to load a Trojan horse image by leveraging shell access, aka Bug ID CSCut67400.	15/12/2015	7.2	CVE-2015-6403
lepide -- active_directory_self_service	The password reset functionality in Lepide Active Directory Self Service allows remote authenticated users to change arbitrary domain user passwords via a crafted request.	15/12/2015	7.4	CVE-2015-8570
xmlsoft -- libxml2	The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.	15/12/2015	7.1	CVE-2015-5312
google -- chrome	The ObjectBackedNativeHandler class in extensions/renderer/object_backed_native_handler.cc in the extensions subsystem in Google Chrome before 47.0.2526.80 improperly implements handler functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."	14/12/2015	10.0	CVE-2015-6788
google -- chrome	Race condition in the MutationObserver implementation in Blink, as used in Google Chrome before 47.0.2526.80, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact by leveraging unanticipated object deletion.	14/12/2015	9.3	CVE-2015-6789
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	14/12/2015	10.0	CVE-2015-6791
google -- chrome	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.80, allow attackers to cause a denial of service or possibly have other impact via unknown vectors, a different issue than CVE-2015-8478.	14/12/2015	10.0	CVE-2015-8548
cisco -- epc3928_docsis_3.0_8x4_wireless_residential	Cisco EPC3928 devices with EDVA 5.5.10, 5.5.11, and 5.7.1 allow remote attackers to bypass an intended authentication requirement and execute unspecified administrative functions via a crafted HTTP request, aka Bug ID CSCux24941.	13/12/2015	7.5	CVE-2015-6401
cisco -- prime_collaboration_assurance	Cisco Prime Collaboration Assurance before 11.0 has a hardcoded cmuser account, which allows remote attackers to obtain access by establishing an SSH session and leveraging knowledge of this account's password, aka Bug ID CSCus62707.	12/12/2015	9.0	CVE-2015-6389
cisco -- unified_computing_system	Cisco Unified Computing System (UCS) 2.2(3f)A on Fabric Interconnect 6200 devices allows remote attackers to cause a denial of service (CPU consumption or device outage) via a SYN flood on the SSH port during the booting process, aka Bug ID CSCuu81757.	12/12/2015	7.1	CVE-2015-6415

Semana 07/12/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	The System Integrity Protection feature in Apple OS X before 10.11.2 mishandles union mounts, which allows attackers to execute arbitrary code in a privileged context via a crafted app with root privileges.	11/12/2015	7.6	CVE-2015-7044
apple -- apple_tv	The kernel in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows local users to gain privileges via a crafted mach message that is misparsed.	11/12/2015	7.2	CVE-2015-7047
apple -- apple_tv	MobileStorageMounter in Apple iOS before 9.2 and tvOS before 9.1 mishandles the timing of trust-cache loading, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	11/12/2015	9.3	CVE-2015-7051
apple -- mac_os_x	kext tools in Apple OS X before 10.11.2 mishandles kernel-extension loading, which allows local users to gain privileges via unspecified vectors.	11/12/2015	7.2	CVE-2015-7052
apple -- apple_tv	AppleMobileFileIntegrity in Apple iOS before 9.2 and tvOS before 9.1 does not prevent changes to access-control structures, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	11/12/2015	9.3	CVE-2015-7055
apple -- mac_os_x	The kernel loader in EFI in Apple OS X before 10.11.2 allows local users to gain privileges via a crafted pathname.	11/12/2015	7.2	CVE-2015-7063
apple -- apple_tv	IOKit SCSI in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via an app that provides an unspecified userclient type.	11/12/2015	9.3	CVE-2015-7068
apple -- iphone_os	Mobile Replayer in GPUTools Framework in Apple iOS before 9.2 allows attackers to execute arbitrary code in a privileged context via an app that provides a crafted pathname, a different vulnerability than CVE-2015-7070.	11/12/2015	9.3	CVE-2015-7069
apple -- iphone_os	Mobile Replayer in GPUTools Framework in Apple iOS before 9.2 allows attackers to execute arbitrary code in a privileged context via an app that provides a crafted pathname, a different vulnerability than CVE-2015-7069.	11/12/2015	9.3	CVE-2015-7070
apple -- mac_os_x	The File Bookmark component in Apple OS X before 10.11.2 allows attackers to bypass a sandbox protection mechanism for app scoped bookmarks via a crafted pathname.	11/12/2015	10.0	CVE-2015-7071
apple -- apple_tv	dyld in Apple iOS before 9.2, tvOS before 9.1, and watchOS before 2.1 mishandles segment validation, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	11/12/2015	9.3	CVE-2015-7072
apple -- mac_os_x	The Intel Graphics Driver component in Apple OS X before 10.11.2 allows local users to gain privileges or cause a denial of service (NULL pointer dereference) via unspecified vectors.	11/12/2015	7.2	CVE-2015-7076
apple -- mac_os_x	The Intel Graphics Driver component in Apple OS X before 10.11.2 allows local users to gain privileges or cause a denial of service (out-of-bounds memory access) via unspecified vectors.	11/12/2015	7.2	CVE-2015-7077
apple -- mac_os_x	Use-after-free vulnerability in Hypervisor in Apple OS X before 10.11.2 allows local users to gain privileges via vectors involving VM objects.	11/12/2015	7.2	CVE-2015-7078
apple -- apple_tv	dyld in Apple iOS before 9.2 and tvOS before 9.1 mishandles segment validation, which allows attackers to execute arbitrary code in a privileged context via a crafted app.	11/12/2015	9.3	CVE-2015-7079
apple -- apple_tv	The kernel in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7084.	11/12/2015	7.2	CVE-2015-7083
apple -- apple_tv	The kernel in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7083.	11/12/2015	7.2	CVE-2015-7084
apple -- mac_os_x	The Intel Graphics Driver component in Apple OS X before 10.11.2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	11/12/2015	7.2	CVE-2015-7106
apple -- mac_os_x	The Bluetooth HCI interface in Apple OS X before 10.11.2 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors.	11/12/2015	7.2	CVE-2015-7108
apple -- iphone_os	IOAcceleratorFamily in Apple OS X before 10.11.2 and tvOS before 9.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	11/12/2015	9.3	CVE-2015-7109
apple -- apple_tv	The IOHIDFamily API in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2015-7112.	11/12/2015	9.3	CVE-2015-7111
apple -- apple_tv	The IOHIDFamily API in Apple iOS before 9.2, OS X before 10.11.2, tvOS before 9.1, and watchOS before 2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2015-7111.	11/12/2015	9.3	CVE-2015-7112
apple -- iphone_os	The LaunchServices component in Apple iOS before 9.2 and watchOS before 2.1 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a malformed plist.	11/12/2015	10.0	CVE-2015-7113
git_project -- git	Multiple unspecified vulnerabilities in Git before 2.5.4, as used in Apple Xcode before 7.2, have unknown impact and attack vectors. NOTE: this CVE is associated only with Xcode use cases.	11/12/2015	10.0	CVE-2015-7082
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8045
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8047
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8048
adobe -- air	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted autoSize property value, a different vulnerability than CVE-2015-8048, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8049
adobe -- air	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted beginGradientFill call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8050
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8055
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8056

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8057
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8058
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8059
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8060
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8061
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8062
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8063
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8064
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8065
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8066
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8067
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8068
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8069

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8070
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8071
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8401
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8402
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8403
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8404
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8405
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8406
adobe -- air	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8457.	10/12/2015	10.0	CVE-2015-8407
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8408
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8440 and CVE-2015-8453.	10/12/2015	10.0	CVE-2015-8409
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8410
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8411
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8412

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8413
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8414
adobe -- air	Buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors.	10/12/2015	10.0	CVE-2015-8415
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8416
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8417
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8418
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8419
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8420
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8421
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8422
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8423
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8424
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8425
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8426
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8427

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8428
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8429
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8430
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8431
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8432
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8433
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8434
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8435
adobe -- air	Use-after-free vulnerability in the PrintJob object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted addPage arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8436
adobe -- air	Use-after-free vulnerability in the Selection object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted setFocus call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8437
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted XML object that is mishandled during a toString call, a different vulnerability than CVE-2015-8446.	10/12/2015	9.3	CVE-2015-8438
adobe -- air	The SharedObject object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code by leveraging an unspecified "type confusion" during a getRemote call, a different vulnerability than CVE-2015-8456.	10/12/2015	9.3	CVE-2015-8439
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8409 and CVE-2015-8453.	10/12/2015	10.0	CVE-2015-8440
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8441
adobe -- air	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8442

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8443
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8451, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8444
adobe -- air	Integer overflow in the Shader filter implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a large BitmapData source object.	10/12/2015	9.3	CVE-2015-8445
adobe -- air	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via an MP3 file with COMM tags that are mishandled during memory allocation, a different vulnerability than CVE-2015-8438.	10/12/2015	9.3	CVE-2015-8446
adobe -- air	Use-after-free vulnerability in the Color object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted setTransform arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8447
adobe -- air	Use-after-free vulnerability in the DisplacementMapFilter object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted mapBitmap property value, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8448
adobe -- air	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted lineTo method call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8449
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value in a TextField object, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8452, and CVE-2015-8454.	10/12/2015	9.3	CVE-2015-8450
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, and CVE-2015-8455.	10/12/2015	10.0	CVE-2015-8451
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8454.	10/12/2015	10.0	CVE-2015-8452
adobe -- air	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8452.	10/12/2015	10.0	CVE-2015-8454
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, and CVE-2015-8451.	10/12/2015	10.0	CVE-2015-8455
adobe -- air	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-8439.	10/12/2015	9.3	CVE-2015-8456
adobe -- air	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8407.	10/12/2015	10.0	CVE-2015-8457
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6040
microsoft -- internet_explorer	Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6151.	09/12/2015	9.3	CVE-2015-6083
microsoft -- live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6106
microsoft -- live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, Windows 10 Gold and 1511, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2010, Lync 2013 SP1, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6107
microsoft -- .net_framework	The Windows font library in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT Gold and 8.1; Office 2007 SP3; Office 2010 SP2; Word Viewer; .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, and 4.6; Skype for Business 2016; Lync 2010; Lync 2013 SP1; Live Meeting 2007 Console; and Silverlight 5 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Graphics Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6108
microsoft -- office	Microsoft Office 2007 SP3 and Office 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6118
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel for Mac 2011, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6122
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6124
microsoft -- windows_server_2008	Use-after-free vulnerability in the DNS server in Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted requests, aka "Windows DNS Use After Free Vulnerability."	09/12/2015	9.3	CVE-2015-6125
microsoft -- windows_10	Race condition in the Pragmatic General Multicast (PGM) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application, aka "Windows PGM UAF Elevation of Privilege Vulnerability."	09/12/2015	7.2	CVE-2015-6126
microsoft -- windows_7	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Windows Library Loading Remote Code Execution Vulnerability."	09/12/2015	7.2	CVE-2015-6128
microsoft -- windows_7	Integer underflow in Uniscribe in Microsoft Windows 7 SP1 and Windows Server 2008 R2 SP1 allows remote attackers to execute arbitrary code via a crafted font, aka "Windows Integer Underflow Vulnerability."	09/12/2015	9.3	CVE-2015-6130
microsoft -- windows_7	Windows Media Center in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8, and Windows 8.1 allows remote attackers to execute arbitrary code via a crafted .mcl file, aka "Media Center Library Parsing RCE Vulnerability."	09/12/2015	9.3	CVE-2015-6131

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Windows Library Loading Remote Code Execution Vulnerability."	09/12/2015	7.2	CVE-2015-6132
microsoft -- windows_10	Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 mishandle library loading, which allows local users to gain privileges via a crafted application, aka "Windows Library Loading Remote Code Execution Vulnerability."	09/12/2015	7.2	CVE-2015-6133
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," a different vulnerability than CVE-2015-6141.	09/12/2015	9.3	CVE-2015-6134
microsoft -- jscript	The Microsoft (1) VBScript 5.7 and 5.8 and (2) JScript 5.7 and 5.8 engines, as used in Internet Explorer 8 through 11 and other products, allow remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6136
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge mishandle content types, which allows remote attackers to execute arbitrary web script in a privileged context via a crafted web site, aka "Microsoft Browser Elevation of Privilege Vulnerability."	09/12/2015	9.3	CVE-2015-6139
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6140
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," a different vulnerability than CVE-2015-6134.	09/12/2015	9.3	CVE-2015-6141
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6142
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-2015-6140, CVE-2015-6142, CVE-2015-6153, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6143
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," a different vulnerability than CVE-2015-6146.	09/12/2015	9.3	CVE-2015-6145
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," a different vulnerability than CVE-2015-6145.	09/12/2015	9.3	CVE-2015-6146
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-2015-6149.	09/12/2015	9.3	CVE-2015-6147
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6156.	09/12/2015	9.3	CVE-2015-6148
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-2015-6147.	09/12/2015	9.3	CVE-2015-6149
microsoft -- internet_explorer	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6154.	09/12/2015	9.3	CVE-2015-6150
microsoft -- edge	Microsoft Internet Explorer 8 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6083.	09/12/2015	9.3	CVE-2015-6151
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," a different vulnerability than CVE-2015-6162.	09/12/2015	9.3	CVE-2015-6152
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6158, CVE-2015-6159, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6153
microsoft -- edge	Microsoft Internet Explorer 7 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6150.	09/12/2015	9.3	CVE-2015-6154
microsoft -- edge	Microsoft Internet Explorer 10 and 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6155
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-2015-6148.	09/12/2015	9.3	CVE-2015-6156
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6159, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6158
microsoft -- edge	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, and CVE-2015-6160.	09/12/2015	9.3	CVE-2015-6159
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-2015-6140, CVE-2015-6142, CVE-2015-6143, CVE-2015-6153, CVE-2015-6158, and CVE-2015-6159.	09/12/2015	9.3	CVE-2015-6160
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," a different vulnerability than CVE-2015-6152.	09/12/2015	9.3	CVE-2015-6162
microsoft -- silverlight	Microsoft Silverlight 5 before 5.1.41105.00 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read or write access) via unspecified open and close requests, aka "Microsoft Silverlight RCE Vulnerability."	09/12/2015	9.3	CVE-2015-6166
microsoft -- edge	Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Edge Memory Corruption Vulnerability," a different vulnerability than CVE-2015-6153.	09/12/2015	9.3	CVE-2015-6168
microsoft -- windows_10	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6173 and CVE-2015-6174.	09/12/2015	7.2	CVE-2015-6171
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2016, Word 2013 RT SP1, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code via a crafted email message processed by Outlook, aka "Microsoft Office RCE Vulnerability."	09/12/2015	9.3	CVE-2015-6172
microsoft -- windows_10	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6171 and CVE-2015-6174.	09/12/2015	7.2	CVE-2015-6173
microsoft -- windows_10	The kernel in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability," a different vulnerability than CVE-2015-6171 and CVE-2015-6173.	09/12/2015	7.2	CVE-2015-6174
microsoft -- windows_10	The kernel in Microsoft Windows 10 Gold allows local users to gain privileges via a crafted application, aka "Windows Kernel Memory Elevation of Privilege Vulnerability."	09/12/2015	7.2	CVE-2015-6175
microsoft -- excel	Microsoft Excel 2007 SP3, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	09/12/2015	9.3	CVE-2015-6177
google -- android	mediaserver in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bugs 24630158 and 23882800, a different vulnerability than CVE-2015-8505, CVE-2015-8506, and CVE-2015-8507.	08/12/2015	9.3	CVE-2015-6616
google -- android	Skia, as used in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23648740.	08/12/2015	9.3	CVE-2015-6617
google -- android	The kernel in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows attackers to gain privileges via a crafted application, aka internal bug 23520714.	08/12/2015	9.3	CVE-2015-6619
google -- android	libstagefright in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bugs 24123723 and 24445127.	08/12/2015	9.3	CVE-2015-6620
google -- android	SystemUI in Android 5.x before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 23909438.	08/12/2015	9.3	CVE-2015-6621
google -- android	Wi-Fi in Android 6.0 before 2015-12-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 24872703.	08/12/2015	9.3	CVE-2015-6623
google -- android	The display drivers in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 23987307.	08/12/2015	9.3	CVE-2015-6633
google -- android	The display drivers in Android before 5.1.1 LMY48Z allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 24163261.	08/12/2015	9.3	CVE-2015-6634
google -- android	mediaserver in Android before 5.1.1 LMY48Z allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 17769851, a different vulnerability than CVE-2015-6616, CVE-2015-8506, and CVE-2015-8507.	08/12/2015	9.3	CVE-2015-8505
google -- android	mediaserver in Android before 5.1.1 LMY48Z and 6.0 before 2015-12-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 24441553, a different vulnerability than CVE-2015-6616, CVE-2015-8505, and CVE-2015-8507.	08/12/2015	9.3	CVE-2015-8506
google -- android	mediaserver in Android 6.0 before 2015-12-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 24157524, a different vulnerability than CVE-2015-6616, CVE-2015-8505, and CVE-2015-8506.	08/12/2015	9.3	CVE-2015-8507
canonical -- lxcfs	The do_write_pids function in lxcfs.c in LXCFS before 0.12 does not properly check permissions, which allows local users to gain privileges by writing a pid to the tasks file.	07/12/2015	7.2	CVE-2015-1344
f5 -- big-ip_access_policy_manager	The iControl API in F5 BIG-IP LTM, AFM, Analytics, APM, ASM, Link Controller, and PEM 11.3.0 before 11.5.3 HF2 and 11.6.0 before 11.6.0 HF6, BIG-IP AAM 11.4.0 before 11.5.3 HF2 and 11.6.0 before 11.6.0 HF6, BIG-IP Edge Gateway, WebAccelerator, and WOM 11.3.0, BIG-IP GTM 11.3.0 before 11.6.0 HF6, BIG-IP PSM 11.3.0 through 11.4.1, Enterprise Manager 3.1.0 through 3.1.1, BIG-IQ Cloud and Security 4.0.0 through 4.5.0, BIG-IQ Device 4.2.0 through 4.5.0, and BIG-IQ ADC 4.5.0 allows remote authenticated users with the "Resource Administrator" role to gain privileges via an iCall (1) script or (2) handler in a SOAP request to iControl/iControlPortal.cgi.	07/12/2015	9.0	CVE-2015-3628
huawei -- unified_security_gateway_firmware	Huawei USG5500, USG2100, USG2200, and USG5100 unified security gateways with software before V300R001C10SPC600, when "DHCP Snooping" is enabled and either "option82 insert" or "option82 rebuild" is enabled on an interface, allow remote attackers to cause a denial of service (reboot) via crafted DHCP packets.	07/12/2015	7.1	CVE-2015-8084
sensiolabs -- symfony	Symfony 2.3.x before 2.3.35, 2.6.x before 2.6.12, and 2.7.x before 2.7.7 might allow remote attackers to have unspecified impact via a timing attack involving the (1) Symfony/Component/Security/Http/RememberMe/PersistentTokenBasedRememberMeServices or (2) Symfony/Component/Security/Http/Firewall/DigestAuthenticationListener class in the Symfony Security Component, or (3) legacy CSRF implementation from the Symfony/Component/Form/Extension/Csrf/CsrfProvider/DefaultCsrfProvider class in the Symfony Form component.	07/12/2015	7.5	CVE-2015-8125
google -- chrome	The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.	05/12/2015	7.5	CVE-2015-6764

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use-after-free vulnerability in content/browser/appcache/appcache_update_job.cc in Google Chrome before 47.0.2526.73 allows remote attackers to execute arbitrary code or cause a denial of service by leveraging the mishandling of AppCache update jobs.	05/12/2015	10.0	CVE-2015-6765
google -- chrome	Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers with renderer access to cause a denial of service or possibly have unspecified other impact by leveraging incorrect AppCacheUpdateJob behavior associated with duplicate cache selection.	05/12/2015	7.5	CVE-2015-6766
google -- chrome	Use-after-free vulnerability in content/browser/appcache/appcache_dispatcher_host.cc in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect pointer maintenance associated with certain callbacks.	05/12/2015	7.5	CVE-2015-6767
google -- chrome	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6770.	05/12/2015	7.5	CVE-2015-6768
google -- chrome	The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.	05/12/2015	7.5	CVE-2015-6769
google -- chrome	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.	05/12/2015	7.5	CVE-2015-6770
google -- chrome	js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.	05/12/2015	7.5	CVE-2015-6771
google -- chrome	The DOM implementation in Blink, as used in Google Chrome before 47.0.2526.73, does not prevent javascript: URL navigation while a document is being detached, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that improperly interacts with a plugin.	05/12/2015	7.5	CVE-2015-6772
google -- chrome	The convolution implementation in Skia, as used in Google Chrome before 47.0.2526.73, does not properly constrain row lengths, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted graphics data.	05/12/2015	7.5	CVE-2015-6773
google -- chrome	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that modifies a pointer used for reporting loadTimes data.	05/12/2015	7.5	CVE-2015-6774
google -- chrome	fpdfsdk/src/jsapi/fxjs_v8.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, does not use signatures, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."	05/12/2015	7.5	CVE-2015-6775
google -- chrome	Use-after-free vulnerability in the ContainerNode::notifyNodeInsertedInternal function in WebKit/Source/core/dom/ContainerNode.cpp in the DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOMCharacterDataModified events for certain detached-subtree insertions.	05/12/2015	7.5	CVE-2015-6777
google -- chrome	The CJBig2_SymbolDict class in fxcodec/jbig2/JBig2_SymbolDict.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a PDF document containing crafted data with JBIG2 compression.	05/12/2015	7.5	CVE-2015-6778
google -- chrome	Integer overflow in the FontData::Bound function in data/font_data.cc in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted offset or length value within font data in an SFNT container.	05/12/2015	7.5	CVE-2015-6781
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.73 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	05/12/2015	10.0	CVE-2015-6787
google -- chrome	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.73, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	05/12/2015	7.5	CVE-2015-8478
google -- chrome	Use-after-free vulnerability in the AudioOutputDevice::OnDeviceAuthorized function in media/audio/audio_output_device.cc in Google Chrome before 47.0.2526.73 allows attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering access to an unauthorized audio output device.	05/12/2015	7.5	CVE-2015-8479
google -- chrome	The VideoFramePool::PoolImpl::CreateFrame function in media/base/video_frame_pool.cc in Google Chrome before 47.0.2526.73 does not initialize memory for a video-frame data structure, which might allow remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact by leveraging improper interaction with the vp3_h_loop_filter_c function in libavcodec/vp3dsp.c in FFmpeg.	05/12/2015	10.0	CVE-2015-8480
cisco -- unified_sip_phone_3900_firmware	Cisco Unified SIP 3905 phones allow remote attackers to cause a denial of service (resource consumption and functionality loss) via a large amount of network traffic, aka Bug ID CSCuh51331.	04/12/2015	7.8	CVE-2015-6391
emc -- networker	EMC NetWorker before 8.0.4.5, 8.1.x before 8.1.3.6, 8.2.x before 8.2.2.2, and 9.0 before build 407 allows remote attackers to cause a denial of service (process outage) via malformed RPC authentication messages.	04/12/2015	7.8	CVE-2015-6849

Semana 30/11/2015

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cyrus -- imap	The index_urlfetch function in index.c in Cyrus IMAP 2.3.x before 2.3.19, 2.4.x before 2.4.18, 2.5.x before 2.5.4 allows remote attackers to obtain sensitive information or possibly have unspecified other impact via vectors related to the urlfetch range, which triggers an out-of-bounds heap read.	03/12/2015	7.5	CVE-2015-8076
cyrus -- imap	Integer overflow in the index_urlfetch function in imap/index.c in Cyrus IMAP 2.3.19, 2.4.18, and 2.5.6 allows remote attackers to have unspecified impact via vectors related to urlfetch range checks and the start_octet variable. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8076.	03/12/2015	7.5	CVE-2015-8077
cyrus -- imap	Integer overflow in the index_urlfetch function in imap/index.c in Cyrus IMAP 2.3.19, 2.4.18, and 2.5.6 allows remote attackers to have unspecified impact via vectors related to urlfetch range checks and the section_offset variable. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8076.	03/12/2015	7.5	CVE-2015-8078
debian -- debian_linux	The Debian build procedure for the smokeping package in wheezy before 2.6.8-2+deb7u1 and jessie before 2.6.9-1+deb8u1 does not properly configure the way Apache httpd passes arguments to smokeping_cgi, which allows remote attackers to execute arbitrary code via crafted CGI arguments.	03/12/2015	7.5	CVE-2015-0859
debian -- dpkg	Off-by-one error in the extracthalf function in dpkg-deb/extract.c in the dpkg-deb component in Debian dpkg 1.16.x before 1.16.17 and 1.17.x before 1.17.26 allows remote attackers to execute arbitrary code via the archive magic version number in an "old-style" Debian binary package, which triggers a stack-based buffer overflow.	03/12/2015	7.5	CVE-2015-0860
cisco -- ios_xe	Cisco IOS XE 15.4(3)S on ASR 1000 devices improperly loads software packages, which allows local users to bypass license restrictions and obtain certain root privileges by using the CLI to enter crafted filenames, aka Bug ID CSCuv93130.	02/12/2015	7.2	CVE-2015-6383
mcafee -- mcafee_enterprise_security_manager	McAfee Enterprise Security Manager (ESM), Enterprise Security Manager/Log Manager (ESMLM), and Enterprise Security Manager/Receiver (ESMREC) 9.3.x before 9.3.2MR19, 9.4.x before 9.4.2MR9, and 9.5.x before 9.5.0MR8, when configured to use Active Directory or LDAP authentication sources, allow remote attackers to bypass authentication by logging in with the username "NGCP|NGCP|NGCP;" and any password.	02/12/2015	9.3	CVE-2015-8024
cisco -- ios	The publish-event event-manager feature in Cisco IOS 15.5(2)S and 15.5(3)S on Cloud Services Router 1000V devices allows local users to execute arbitrary commands with root privileges by leveraging administrative access to enter crafted environment variables, aka Bug ID CSCux14943.	01/12/2015	7.2	CVE-2015-6385
pcre -- perl_compatible_regular_expression_library	PCRE before 8.36 mishandles the /(((a)|(a*)\g<-1>))*/ pattern and related patterns with certain internal recursive back references, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-2327
pcre -- perl_compatible_regular_expression_library	PCRE before 8.36 mishandles the /((?(R)a|(?1)))+/ pattern and related patterns with certain recursion, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-2328
pcre -- perl_compatible_regular_expression_library	The pcre_exec function in pcre_exec.c in PCRE before 8.38 mishandles a // pattern with a 1 string, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8380
pcre -- perl_compatible_regular_expression_library	The compile_regex function in pcre_compile.c in PCRE before 8.38 and pcre2_compile.c in PCRE2 before 10.2x mishandles the /(?J:(?|(:(?|(?'R')(\k'R')|((?'R')))H'Rk'Rf)|s(?'R'))))/ and /(?J:(?|(:(?|(?'R')(\z(?|(?'R')(\k'R')|((?'R')))k'R')|((?'R')))H'Ak'Rf)|s(?'R')))/ patterns, and related patterns with certain group references, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8381
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles certain repeated conditional groups, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8383
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the /(?J)(?'d'(?'d'\g{d}))/ pattern and related patterns with certain recursive back references, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8392 and CVE-2015-8395.	01/12/2015	7.5	CVE-2015-8384
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the /(?|(\k'Pm')|(?'Pm'))/ pattern and related patterns with certain forward references, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8385
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8386
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles (?123) subroutine calls and related subroutine calls, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8387
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the /(?=di(?<=(?1))|(?=(.))))/ pattern and related patterns with an unmatched closing parenthesis, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8388
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the /(?:|a|){100}x/ pattern and related patterns, which allows remote attackers to cause a denial of service (infinite recursion) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8389
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the [: and \ substrings in character classes, which allows remote attackers to cause a denial of service (uninitialized memory read) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8390
pcre -- perl_compatible_regular_expression_library	The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [: nesting, which allows remote attackers to cause a denial of service (CPU consumption) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	9.0	CVE-2015-8391
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles certain instances of the (?| substring, which allows remote attackers to cause a denial of service (unintended recursion and buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8384 and CVE-2015-8395.	01/12/2015	7.5	CVE-2015-8392
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles the (?(<digits>) and (?(R<digits>) conditions, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	01/12/2015	7.5	CVE-2015-8394
pcre -- perl_compatible_regular_expression_library	PCRE before 8.38 mishandles certain references, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8384 and CVE-2015-8392.	01/12/2015	7.5	CVE-2015-8395