Henson Scap

Details of Vulnerabilties as of 2013-12-16 for 'linux'

See next page

# Of Vuls	CVE-ID	Summary	Vulnerable Software

# Of Vuls	CVE-ID	Summary	Vulnerable Software
1	CVE-2013-4470	The Linux kernel before 3.12, when UDP Fragmentation Offload (UFO) is enabled, does not properly initialize certain data structures, which allows local users to cause a denial of service (memory corruption and system crash) or possibly gain privileges via a crafted application that uses the UDP_CORK option in a setsockopt system call and sends both short and long packets, related to the ip_ufo_append_data function in net/ipv4/ip_output.c and the ip6_ufo_append_data function in net/ipv6/ip6_output.c.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.10.12", "cpe:/o:linux:linux_kernel:3.10.13", "cpe:/o:linux:linux_kernel:3.10.14", "cpe:/o:linux:linux_kernel:3.10.10", "cpe:/o:linux:linux_kernel:3.10.11", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.10.17", "cpe:/o:linux:linux_kernel:3.10.16", "cpe:/o:linux:linux_kernel:3.10.18", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.10.15", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.11.1", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.11.2", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4:rc3:~~~~x86~", "cpe:/o:linux:linux_kernel:3.4:rc2:~~~~x86~", "cpe:/o:linux:linux_kernel:3.4:rc1:~~~~x86~",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
2	CVE-2013-6392	The genlock_dev_ioctl function in genlock.c in the Genlock driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted GENLOCK_IOC_EXPORT ioctl call.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.10.12", "cpe:/o:linux:linux_kernel:3.10.13", "cpe:/o:linux:linux_kernel:3.10.14", "cpe:/o:linux:linux_kernel:3.10.10", "cpe:/o:linux:linux_kernel:3.10.11", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.10.17", "cpe:/o:linux:linux_kernel:3.10.16", "cpe:/o:linux:linux_kernel:3.10.18", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.10.15", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.11.1", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.11.2", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4:rc3:~~~~x86~", "cpe:/o:linux:linux_kernel:3.4:rc2:~~~~x86~", "cpe:/o:linux:linux_kernel:3.4:rc1:~~~~x86~",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
3	CVE-2013-4387	net/ipv6/ip6_output.c in the Linux kernel through 3.11.4 does not properly determine the need for UDP Fragmentation Offload (UFO) processing of small packets after the UFO queueing of a large packet, which allows remote attackers to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact via network traffic that triggers a large response packet.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.10.12", "cpe:/o:linux:linux_kernel:3.10.10", "cpe:/o:linux:linux_kernel:3.10.11", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.11.1", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.11.2", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4:rc3:~~~~x86~", "cpe:/o:linux:linux_kernel:3.4.30", "cpe:/o:linux:linux_kernel:3.4.31", "cpe:/o:linux:linux_kernel:3.4.32", "cpe:/o:linux:linux_kernel:3.0.64", "cpe:/o:linux:linux_kernel:3.11", "cpe:/o:linux:linux_kernel:3.0.62", "cpe:/o:linux:linux_kernel:3.0.63", "cpe:/o:linux:linux_kernel:3.0.60",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
4	CVE-2013-4299	Interpretation conflict in drivers/md/dm-snap-persistent.c in the Linux kernel through 3.11.6 allows remote authenticated users to obtain sensitive information or modify data via a crafted mapping to a snapshot block device.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.10.12", "cpe:/o:linux:linux_kernel:3.10.10", "cpe:/o:linux:linux_kernel:3.10.11", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.11.1", "cpe:/o:linux:linux_kernel:3.11.2", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4.30", "cpe:/o:linux:linux_kernel:3.4.31", "cpe:/o:linux:linux_kernel:3.4.32", "cpe:/o:linux:linux_kernel:3.11", "cpe:/o:linux:linux_kernel:3.0.64", "cpe:/o:linux:linux_kernel:3.0.62", "cpe:/o:linux:linux_kernel:3.0.63", "cpe:/o:linux:linux_kernel:3.0.60", "cpe:/o:linux:linux_kernel:3.0.61",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
5	CVE-2013-4350	The IPv6 SCTP implementation in net/sctp/ipv6.c in the Linux kernel through 3.11.1 uses data structures and function calls that do not trigger an intended configuration of IPsec encryption, which allows remote attackers to obtain sensitive information by sniffing the network.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.10.12", "cpe:/o:linux:linux_kernel:3.10.10", "cpe:/o:linux:linux_kernel:3.10.11", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.11.1", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4.30", "cpe:/o:linux:linux_kernel:3.4.31", "cpe:/o:linux:linux_kernel:3.4.32", "cpe:/o:linux:linux_kernel:3.11", "cpe:/o:linux:linux_kernel:3.0.64", "cpe:/o:linux:linux_kernel:3.0.62", "cpe:/o:linux:linux_kernel:3.0.63", "cpe:/o:linux:linux_kernel:3.0.60", "cpe:/o:linux:linux_kernel:3.0.61", "cpe:/o:linux:linux_kernel:3.10.4",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
6	CVE-2013-4162	The udp_v6_push_pending_frames function in net/ipv6/udp.c in the IPv6 implementation in the Linux kernel through 3.10.3 makes an incorrect function call for pending data, which allows local users to cause a denial of service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt system call.	["cpe:/o:linux:linux_kernel:3.2.11", "cpe:/o:linux:linux_kernel:3.2.10", "cpe:/o:linux:linux_kernel:3.2.12", "cpe:/o:linux:linux_kernel:3.2.19", "cpe:/o:linux:linux_kernel:3.2.18", "cpe:/o:linux:linux_kernel:3.2.17", "cpe:/o:linux:linux_kernel:3.2.16", "cpe:/o:linux:linux_kernel:3.2.15", "cpe:/o:linux:linux_kernel:3.2.14", "cpe:/o:linux:linux_kernel:3.2.13", "cpe:/o:linux:linux_kernel:3.0.29", "cpe:/o:linux:linux_kernel:3.0.30", "cpe:/o:linux:linux_kernel:3.0.31", "cpe:/o:linux:linux_kernel:3.0.38", "cpe:/o:linux:linux_kernel:3.0.37", "cpe:/o:linux:linux_kernel:3.0.39", "cpe:/o:linux:linux_kernel:3.0.34", "cpe:/o:linux:linux_kernel:3.6.10", "cpe:/o:linux:linux_kernel:3.0.33", "cpe:/o:linux:linux_kernel:3.0.36", "cpe:/o:linux:linux_kernel:3.0.35", "cpe:/o:linux:linux_kernel:3.6.11", "cpe:/o:linux:linux_kernel:3.0.32", "cpe:/o:linux:linux_kernel:3.0.19", "cpe:/o:linux:linux_kernel:3.4.30", "cpe:/o:linux:linux_kernel:3.4.31", "cpe:/o:linux:linux_kernel:3.4.32", "cpe:/o:linux:linux_kernel:3.0.64", "cpe:/o:linux:linux_kernel:3.0.62", "cpe:/o:linux:linux_kernel:3.0.63", "cpe:/o:linux:linux_kernel:3.0.60", "cpe:/o:linux:linux_kernel:3.0.61", "cpe:/o:linux:linux_kernel:3.0.68", "cpe:/o:linux:linux_kernel:3.0.67", "cpe:/o:linux:linux_kernel:3.0.66", "cpe:/o:linux:linux_kernel:3.0.65", "cpe:/o:linux:linux_kernel:3.2:rc2", "cpe:/o:linux:linux_kernel:3.1:rc1",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
7	CVE-2013-2825	The DNP3 service in the Outstation component on Elecsys Director Gateway devices with kernel 2.6.32.11ael1 and earlier allows remote attackers to cause a denial of service (CPU consumption and communication outage) via crafted input.	cpe:/h:elecsyscorp:director_industrial_communication_gateway:-
8	CVE-2013-2850	Heap-based buffer overflow in the iscsi_add_notunderstood_response function in drivers/target/iscsi/iscsi_target_parameters.c in the iSCSI target subsystem in the Linux kernel through 3.9.4 allows remote attackers to cause a denial of service (memory corruption and OOPS) or possibly execute arbitrary code via a long key that is not properly handled during construction of an error-response packet.	["cpe:/o:linux:linux_kernel:3.9:rc7", "cpe:/o:linux:linux_kernel:3.9.4", "cpe:/o:linux:linux_kernel:3.9.0", "cpe:/o:linux:linux_kernel:3.9.3", "cpe:/o:linux:linux_kernel:3.9.2", "cpe:/o:linux:linux_kernel:3.9.1", "cpe:/o:linux:linux_kernel:3.9:rc2", "cpe:/o:linux:linux_kernel:3.9:rc1", "cpe:/o:linux:linux_kernel:3.9:rc6", "cpe:/o:linux:linux_kernel:3.9:rc5", "cpe:/o:linux:linux_kernel:3.9:rc4", "cpe:/o:linux:linux_kernel:3.9:rc3"]
9	CVE-2013-6431	The fib6_add function in net/ipv6/ip6_fib.c in the Linux kernel before 3.11.5 does not properly implement error-code encoding, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability for an IPv6 SIOCADDRT ioctl call.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
10	CVE-2012-5612	Heap-based buffer overflow in Oracle MySQL 5.5.19 and other versions through 5.5.28, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code, as demonstrated using certain variations of the (1) USE, (2) SHOW TABLES, (3) DESCRIBE, (4) SHOW FIELDS FROM, (5) SHOW COLUMNS FROM, (6) SHOW INDEX FROM, (7) CREATE TABLE, (8) DROP TABLE, (9) ALTER TABLE, (10) DELETE FROM, (11) UPDATE, and (12) SET PASSWORD commands.	["cpe:/a:mariadb:mariadb:5.5.28a", "cpe:/a:oracle:mysql:5.5.19"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
11	CVE-2012-5611	Stack-based buffer overflow in the acl_get function in Oracle MySQL 5.5.19 and other versions through 5.5.28, and 5.1.53 and other versions through 5.1.66, and MariaDB 5.5.2.x before 5.5.28a, 5.3.x before 5.3.11, 5.2.x before 5.2.13 and 5.1.x before 5.1.66, allows remote authenticated users to execute arbitrary code via a long argument to the GRANT FILE command.	["cpe:/a:mariadb:mariadb:5.2.8", "cpe:/a:mariadb:mariadb:5.2.9", "cpe:/a:mariadb:mariadb:5.2.6", "cpe:/a:mariadb:mariadb:5.2.7", "cpe:/a:mariadb:mariadb:5.2.5", "cpe:/a:mariadb:mariadb:5.3.10", "cpe:/a:mariadb:mariadb:5.3.0", "cpe:/a:mariadb:mariadb:5.1.47", "cpe:/a:mariadb:mariadb:5.3.2", "cpe:/a:mariadb:mariadb:5.3.1", "cpe:/a:mariadb:mariadb:5.2.2", "cpe:/a:mariadb:mariadb:5.2.3", "cpe:/a:mariadb:mariadb:5.2.0", "cpe:/a:mariadb:mariadb:5.1.49", "cpe:/a:mariadb:mariadb:5.2.1", "cpe:/a:mariadb:mariadb:5.5.25", "cpe:/a:mariadb:mariadb:5.5.24", "cpe:/a:mariadb:mariadb:5.5.23", "cpe:/a:mariadb:mariadb:5.5.22", "cpe:/a:mariadb:mariadb:5.2.10", "cpe:/a:mariadb:mariadb:5.5.21", "cpe:/a:mariadb:mariadb:5.2.12", "cpe:/a:mariadb:mariadb:5.5.20", "cpe:/a:mariadb:mariadb:5.2.11", "cpe:/a:oracle:mysql:5.1.53", "cpe:/a:mariadb:mariadb:5.1.55", "cpe:/a:mariadb:mariadb:5.3.5", "cpe:/a:mariadb:mariadb:5.3.6", "cpe:/a:mariadb:mariadb:5.1.53", "cpe:/a:mariadb:mariadb:5.3.4", "cpe:/a:mariadb:mariadb:5.1.61", "cpe:/a:mariadb:mariadb:5.1.51", "cpe:/a:mariadb:mariadb:5.3.9", "cpe:/a:mariadb:mariadb:5.1.62", "cpe:/a:mariadb:mariadb:5.1.50", "cpe:/a:mariadb:mariadb:5.3.7", "cpe:/a:mariadb:mariadb:5.1.60", "cpe:/a:mariadb:mariadb:5.5.27", "cpe:/a:mariadb:mariadb:5.3.8", "cpe:/a:mariadb:mariadb:5.1.41", "cpe:/a:mariadb:mariadb:5.1.42", "cpe:/a:mariadb:mariadb:5.5.28", "cpe:/a:mariadb:mariadb:5.3.3", "cpe:/a:mariadb:mariadb:5.1.44", "cpe:/a:mariadb:mariadb:5.2.4", "cpe:/a:oracle:mysql:5.5.19"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
12	CVE-2013-2930	The perf_trace_event_perm function in kernel/trace/trace_event_perf.c in the Linux kernel before 3.12.2 does not properly restrict access to the perf subsystem, which allows local users to enable function tracing via a crafted application.	No software given
13	CVE-2013-4270	The net_ctl_permissions function in net/sysctl_net.c in the Linux kernel before 3.11.5 does not properly determine uid and gid values, which allows local users to bypass intended /proc/sys/net restrictions via a crafted application.	No software given
14	CVE-2013-7027	The ieee80211_radiotap_iterator_init function in net/wireless/radiotap.c in the Linux kernel before 3.11.7 does not check whether a frame contains any data outside of the header, which might allow attackers to cause a denial of service (buffer over-read) via a crafted header.	No software given
15	CVE-2013-2929	The Linux kernel before 3.12.2 does not properly use the get_dumpable function, which allows local users to bypass intended ptrace restrictions or obtain sensitive information from IA64 scratch registers via a crafted application, related to kernel/ptrace.c and arch/ia64/include/asm/processor.h.	No software given
16	CVE-2013-7026	Multiple race conditions in ipc/shm.c in the Linux kernel before 3.12.2 allow local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted application that uses shmctl IPC_RMID operations in conjunction with other shm system calls.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
17	CVE-2013-6432	The ping_recvmsg function in net/ipv4/ping.c in the Linux kernel before 3.12.4 does not properly interact with read system calls on ping sockets, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging unspecified privileges to execute a crafted application.	No software given
18	CVE-2011-2729	native/unix/native/jsvc-unix.c in jsvc in the Daemon component 1.0.3 through 1.0.6 in Apache Commons, as used in Apache Tomcat 5.5.32 through 5.5.33, 6.0.30 through 6.0.32, and 7.0.x before 7.0.20 on Linux, does not drop capabilities, which allows remote attackers to bypass read permissions for files via a request to an application.	["cpe:/a:apache:tomcat:6.0.31", "cpe:/a:apache:tomcat:6.0.30", "cpe:/a:apache:tomcat:6.0.32", "cpe:/a:apache:tomcat:5.5.33", "cpe:/a:apache:tomcat:5.5.32", "cpe:/a:apache:tomcat:7.0.6", "cpe:/a:apache:tomcat:7.0.7", "cpe:/a:apache:tomcat:7.0.8", "cpe:/a:apache:tomcat:7.0.19", "cpe:/a:apache:tomcat:7.0.9", "cpe:/a:apache:tomcat:7.0.17", "cpe:/a:apache:tomcat:7.0.16", "cpe:/a:apache:tomcat:7.0.13", "cpe:/a:apache:tomcat:7.0.11", "cpe:/a:apache:tomcat:7.0.12", "cpe:/a:apache:tomcat:7.0.10", "cpe:/a:apache:tomcat:7.0.5", "cpe:/a:apache:tomcat:7.0.4", "cpe:/a:apache:tomcat:7.0.14", "cpe:/a:apache:tomcat:7.0.3", "cpe:/a:apache:tomcat:7.0.2", "cpe:/a:apache:tomcat:7.0.1", "cpe:/a:apache:tomcat:7.0.0:beta", "cpe:/a:apache:tomcat:7.0.0", "cpe:/a:apache:apache_commons_daemon:1.0.3", "cpe:/a:apache:apache_commons_daemon:1.0.6", "cpe:/a:apache:apache_commons_daemon:1.0.5", "cpe:/a:apache:apache_commons_daemon:1.0.4"]

# Of Vuls	CVE-ID	Summary	Vulnerable Software
19	CVE-2013-2728	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
20	CVE-2013-3324	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
21	CVE-2013-3325	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
22	CVE-2013-3326	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
23	CVE-2013-3327	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
24	CVE-2013-3328	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
25	CVE-2013-3329	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
26	CVE-2013-3330	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
27	CVE-2013-3331	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
28	CVE-2013-3332	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
29	CVE-2013-3333	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3334, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
30	CVE-2013-3334	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, and CVE-2013-3335.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
31	CVE-2013-3335	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, and CVE-2013-3334.	["cpe:/a:adobe:flash_player:7.0.19.0", "cpe:/a:adobe:flash_player:7.0.69.0", "cpe:/a:adobe:flash_player:9.0.28", "cpe:/a:adobe:adobe_air:3.5.0.890", "cpe:/a:adobe:flash_player:10.1.102.64", "cpe:/a:adobe:flash_player:10.1.92.8", "cpe:/a:adobe:flash_player:9.0.31.0", "cpe:/a:adobe:flash_player:9.0.20", "cpe:/a:adobe:flash_player:11.3.300.271", "cpe:/a:adobe:flash_player:11.3.300.273", "cpe:/a:adobe:flash_player:9.0.115.0", "cpe:/a:adobe:flash_player:7.0.73.0", "cpe:/a:adobe:adobe_air:3.0.0.408", "cpe:/a:adobe:flash_player:11.3.300.270", "cpe:/a:adobe:flash_player:9.0.31", "cpe:/a:adobe:flash_player:7.2", "cpe:/a:adobe:flash_player:10.2.154.25", "cpe:/a:adobe:flash_player:7.1", "cpe:/a:adobe:flash_player:6.0.21.0", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2540", "cpe:/a:adobe:flash_player:7.0", "cpe:/a:adobe:adobe_air_sdk:3.3.0.3650", "cpe:/a:adobe:flash_player:11.1.102.62", "cpe:/a:adobe:adobe_air:3.0.0.4080", "cpe:/a:adobe:flash_player:11.1.102.63", "cpe:/a:adobe:flash_player:11.1.115.54", "cpe:/a:adobe:adobe_air:3.7.0.1530", "cpe:/a:adobe:flash_player:9.0.125.0", "cpe:/a:adobe:flash_player:7.1.1", "cpe:/a:adobe:flash_player:8.0.24.0", "cpe:/a:adobe:flash_player:11.6.602.167", "cpe:/a:adobe:flash_player:10.1.52.14.1", "cpe:/a:adobe:flash_player:11.6.602.168", "cpe:/a:adobe:adobe_air_sdk:3.5.0.890", "cpe:/a:adobe:adobe_air:3.5.0.600", "cpe:/a:adobe:flash_player:9.0.16", "cpe:/a:adobe:adobe_air_sdk:3.4.0.2710", "cpe:/a:adobe:flash_player:8.0.22.0",

# Of Vuls	CVE-ID	Summary	Vulnerable Software
32	CVE-2012-5615	MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.66, and possibly other versions, generates different error messages with different time delays depending on whether a user name exists, which allows remote attackers to enumerate valid usernames.	["cpe:/a:mariadb:mariadb:5.3.11", "cpe:/a:mariadb:mariadb:5.1.66", "cpe:/a:mariadb:mariadb:5.2.13", "cpe:/a:mariadb:mariadb:5.5.28a", "cpe:/a:oracle:mysql:5.5.19"]
33	CVE-2013-3707	The HTTPSTK service in the novell-nrm package before 2.0.2-297.305.302.3 in Novell Open Enterprise Server 2 (OES 2) Linux, and OES 11 Linux Gold and SP1, does not make the intended SSL_free and SSL_shutdown calls for the close of a TCP connection, which allows remote attackers to cause a denial of service (service crash) by establishing many TCP connections to port 8009.	["cpe:/a:novell:open_enterprise_server:11.0", "cpe:/a:novell:open_enterprise_server:11.0:sp1", "cpe:/a:novell:open_enterprise_server:2"]
34	CVE-2012-0426	Race condition in sap_suse_cluster_connector before 1.0.0-0.8.1 in SUSE Linux Enterprise for SAP Applications 11 SP2 allows local users to have an unspecified impact via vectors related to a tmp/ directory.	cpe:/a:novell:suse_linux_enterprise_for_sap_applications:11:sp2
35	CVE-2012-0414	Cross-site scripting (XSS) vulnerability in the Spacewalk service in SUSE Manager 1.2 for SUSE Linux Enterprise (SLE) 11 SP1 allows remote attackers to inject arbitrary web script or HTML via an image name.	cpe:/a:novell:suse_manager:1.2
36	CVE-2013-6427	upgrade.py in the hp-upgrade service in HP Linux Imaging and Printing (HPLIP) 3.x through 3.13.11 launches a program from an http URL, which allows man-in-the-middle attackers to execute arbitrary code by gaining control over the client-server data stream.	No software given

# Of Vuls	CVE-ID	Summary	Vulnerable Software
37	CVE-2013-4325	The check_permission_v1 function in base/pkit.py in HP Linux Imaging and Printing (HPLIP) through 3.13.9 does not properly use D-Bus for communication with a polkit authority, which allows local users to bypass intended access restrictions by leveraging a PolkitUnixProcess PolkitSubject race condition via a (1) setuid process or (2) pkexec process.	["cpe:/a:hp:linux_imaging_and_printing_project:3.11.1", "cpe:/a:hp:linux_imaging_and_printing_project:3.11.5", "cpe:/a:hp:linux_imaging_and_printing_project:3.11.3", "cpe:/a:hp:linux_imaging_and_printing_project:3.10.2", "cpe:/a:hp:linux_imaging_and_printing_project:2.7.10", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.11", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.10", "cpe:/a:hp:linux_imaging_and_printing_project:3.11.3a", "cpe:/a:hp:linux_imaging_and_printing_project:3.11.7", "cpe:/a:hp:linux_imaging_and_printing_project:1.0", "cpe:/a:hp:linux_imaging_and_printing_project:3.10.9", "cpe:/a:hp:linux_imaging_and_printing_project:3.10.5", "cpe:/a:hp:linux_imaging_and_printing_project:3.11.10", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.10:a", "cpe:/a:hp:linux_imaging_and_printing_project:3.10.6", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.4b", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.4", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.3", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.2", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.2", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.8", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.4", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.7", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.6", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.6", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.5", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.8", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.6", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.9", "cpe:/a:hp:linux_imaging_and_printing_project:3.13.9", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.12", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.2", "cpe:/a:hp:linux_imaging_and_printing_project:3.12.4", "cpe:/a:hp:linux_imaging_and_printing_project:2.0", "cpe:/a:hp:linux_imaging_and_printing_project:3.9.10"]