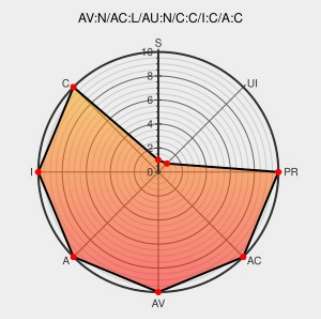
CVE-2013-2555

Published on: 03/11/2013 12:00:00 AM UTC

Last Modified on: 09/08/2021 05:19:00 PM UTC

CVE-2013-2555

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Air from Adobe contain the following vulnerability:

Integer overflow in Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.

CVE-2013-2555 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2013:0670-1: important: Security update for	Mailing List, Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SU-2013:0670
NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	BUGTRAQ 20130418 VUPEN Security Research - Adobe Flash Player RTMP Data Processing Object Confusion (CVE-2013-2555)
'[security bulletin] HPSBMU02948 rev.1 - HP Systems Insight Manager (SIM) Running on Linux and Window' - MARC	Third Party Advisory, marc.info, text/html	HP HPSBMU02948

Pwn2Own 2013 - HP Enterprise Business Community	Permissions Required web.archive.org text/html Inactive Link Not Archived	MISC h30499.www3.hp.com/t5/HP-Security-Research-Blog/Pwn2Own-2013/ba-p/5981157
Adobe - Security Bulletins: APSB13-11 - Security updates for Adobe Flash Player	Vendor Advisory www.adobe.com text/xml	CONFIRM www.adobe.com/support/security/bulletins/apsb13-11.html
[security-announce] openSUSE-SU-2013:0675-1: important: flash-player upd	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0675
JavaScript is not available.	Broken Link nitter.domain.glass text/html	MISC twitter.com/VUPEN/statuses/309713355466227713
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0730
openSUSE-SU-2013:0672-1: moderate: flash-player: update to 11.2.202.280	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0672
Zero Day Initiative na Twitterze: "@VUPEN just took down Adobe Flash for $70k and a grand total of $250k! #pwn2own"	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/thezdi/statuses/309756927301283840

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Air	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All

Operating System	Apple	Mac Os	-	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.4	All	All	All

Operating System	Redhat	Enterprise Linux Eus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All

cpe:2.3:a:adobe:air:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.9:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:5.9:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:5.9:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:5.9:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→