



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 [M](#) 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
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

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
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 →

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)