



CVE-2013-3324

Published on: 05/16/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

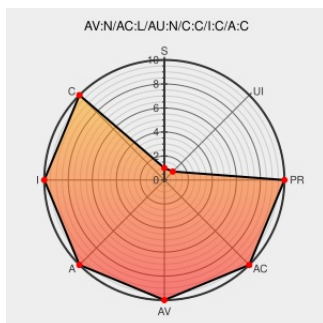
CVE-2013-3324

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Adobe Air](#) from [Adobe](#) contain the following vulnerability:

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.

CVE-2013-3324 has been assigned by psirt@adobe.com 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

Red Hat Customer Portal

[Third Party Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2013:0825](#)

[security-announce] openSUSE-SU-2013:0954-1:
important: flash-player to

[Mailing List](#)

[Third Party Advisory](#)

[lists.opensuse.org](#)

[text/html](#)

[SUSE openSUSE-SU-2013:0954](#)

Security Advisory SA53442 - Microsoft Windows Flash Player Multiple Vulnerabilities - Secunia	Broken Link web.archive.org text/html	 SECUNIA 53442
[security-announce] openSUSE-SU-2013:0892-1: important: flash-player to	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0892
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:16969
[security-announce] SUSE-SU-2013:0798-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2013:0798
Adobe - Security Bulletins: APSB13-14 - Security updates for Adobe Flash Player	Patch Vendor Advisory www.adobe.com text/xml	 CONFIRM www.adobe.com/support/security/bulletins/apsb13-14.html
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	Adobe Air	All	All	All	All
Application	Adobe	Adobe Air	All	All	All	All
Application	Adobe	Adobe Air Sdk	All	All	All	All
Application	Adobe	Adobe Air Sdk	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	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	All
Operating System	Google	Android	All	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	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	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	12.2	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 Eus	5.9	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	5.9	All	All	All

Operating System	Redhat	Enterprise Linux Server Eus	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	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
cpe:2.3:a:adobe:adobe_air:*****:						
cpe:2.3:a:adobe:adobe_air:*****:						
cpe:2.3:a:adobe:adobe_air_sdk:*****:						
cpe:2.3:a:adobe:adobe_air_sdk:*****:						
cpe:2.3:a:adobe:flash_player:*****:						
cpe:2.3:a:adobe:flash_player:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
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:12.2:*****:						

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:
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_eus:5.9:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.4:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus:5.9:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_eus: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:10:sp4:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp4:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)