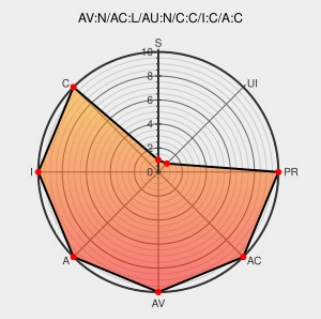
CVE-2013-3343

Published on: 06/11/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:31 PM UTC

CVE-2013-3343

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



Certain versions of Air from Adobe contain the following vulnerability:

Adobe Flash Player before 10.3.183.90 and 11.x before 11.7.700.224 on Windows, before 10.3.183.90 and 11.x before 11.7.700.225 on Mac OS X, before 10.3.183.90 and 11.x before 11.2.202.291 on Linux, before 11.1.111.59 on Android 2.x and 3.x, and before 11.1.115.63 on Android 4.x; Adobe AIR before 3.7.0.2090 on Windows and Android and before 3.7.0.2100 on Mac OS X; and Adobe AIR SDK & Compiler before 3.7.0.2090 on Windows and before 3.7.0.2100 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

CVE-2013-3343 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
Repository / Oval Repository	Technical Description, oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:17030
openSUSE-SU-2013:1040-1: moderate: update for flash-player	Mailing List, Technical Description, lists.opensuse.org, text/html	SUSE openSUSE-SU-2013:1040
[security-announce] SUSE-SU-2013:1039-1: important: Security update for	Mailing List	SUSE SUSE-SU-2013:1039

Security update for	Technical Description lists.opensuse.org text/html	
openSUSE-SU-2013:1063-1: moderate: update for flash-player	Mailing List Technical Description lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1063
Adobe - Security Bulletins: APSB13-16 - Security updates available for Adobe Flash Player	Patch Vendor Advisory www.adobe.com text/xml	CONFIRM www.adobe.com/support/security/bulletins/apsb13-16.html
Red Hat Customer Portal	Technical Description web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0941

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	Air	All	All	All	All
Application	Adobe	Air Sdk	All	All	All	All
Application	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
Operating System	Apple	Mac Os X	-	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	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	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

- cpe:2.3:a:adobe:air:*:*:*:*:*:*:*:*:
- cpe:2.3:a:adobe:air:*:*:*:*:*:*:*:*:
- cpe:2.3:a:adobe:air_sdk:*:*:*:*:*:*:*:*:
- cpe:2.3:a: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: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:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→