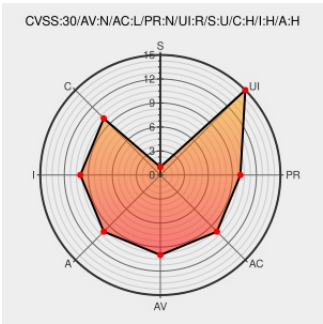
CVE-2015-8634

Published on: 12/28/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8634

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



Certain versions of Air from Adobe contain the following vulnerability:

Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.

CVE-2015-8634 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Document Display | HPE Support Center	[illegible]	CONFIRM

Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05356388
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
Adobe Flash Player Multiple Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034544
Adobe Flash - Use-After-Free When Setting Stage - Windows_x86-64 dos Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39221
[security-announce] SUSE-SU-2015:2401-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2401
[security-announce] openSUSE-SU-2015:2400-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2400
Document Display | HPE Support Center	h20566.www2.hpe.com text/html	CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2697
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	CONFIRM helpx.adobe.com/security/products/flash-player/apsb16-01.html
Adobe Flash Player and AIR APSB16-01 Multiple Use After Free Remote Code Execution Vulnerabilities	cve.report (archive) text/html	BID 79701
[security-announce] openSUSE-SU-2015:2403-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2403
[security-announce] SUSE-SU-2015:2402-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2402

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 Sdk	All	All	All	All
Application	Adobe	Air Sdk Compiler	All	All	All	All
Application	Adobe	Air Sdk Compiler	All	All	All	All
Application	Adobe	Flash Player	19.0.0.185	All	All	All

Application	Adobe	Flash Player	19.0.0.207	All	All	All
Application	Adobe	Flash Player	19.0.0.226	All	All	All
Application	Adobe	Flash Player	19.0.0.245	All	All	All
Application	Adobe	Flash Player	20.0.0.228	All	All	All
Application	Adobe	Flash Player	20.0.0.235	All	All	All
Application	Adobe	Flash Player	19.0.0.185	All	All	All
Application	Adobe	Flash Player	19.0.0.207	All	All	All
Application	Adobe	Flash Player	19.0.0.226	All	All	All
Application	Adobe	Flash Player	19.0.0.245	All	All	All
Application	Adobe	Flash Player	20.0.0.228	All	All	All
Application	Adobe	Flash Player	20.0.0.235	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	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	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

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

cpe:2.3:a:adobe:air_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:air_sdk_&_compiler:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:air_sdk_\&_compiler:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.185:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.207:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.226:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.245:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:20.0.0.228:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:20.0.0.235:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.185:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.207:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.226:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:19.0.0.245:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:20.0.0.228:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:20.0.0.235:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

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: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→

CVE.report and Source URL Uptime Status status.cve.report