

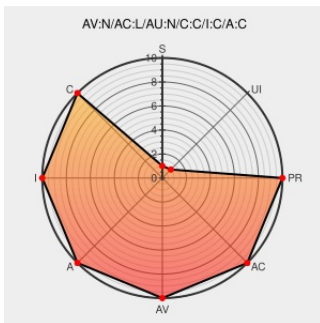


CVE-2015-8416

Published on: 12/09/2015 12:00:00 AM UTC

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

CVE-2015-8416

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-

2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.

CVE-2015-8416 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
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 Security Bulletin	Patch Vendor Advisory helpx.adobe.com	CONFIRM helpx.adobe.com/security/products/flash-player/apsb15-32.html

helpx.adobe.com
text/html

ZDI-15-666 | Zero Day Initiative

www.zerodayinitiative.com
text/html

 MISC www.zerodayinitiative.com/advisories/ZDI-15-666

Adobe Flash Player and AIR APSB15-32
Multiple Unspecified Memory Corruption
Vulnerabilities

cve.report (archive)
text/html

 BID 78710

[security-announce] SUSE-SU-2015:2236-1:
important: Security update for

lists.opensuse.org
text/html

 SUSE [SUSE-SU-2015:2236](https://www.suse.com/support/update/patches/view.php?id=suse-su-2236)

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](http://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680)

Adobe Flash Player: Multiple vulnerabilities
(GLSA 201601-03) — Gentoo Security

security.gentoo.org
text/html

 GENTOO GLSA-201601-03

[security-announce] SUSE-SU-2015:2247-1:
important: Security update for

lists.opensuse.org
text/html

 SUSE [SUSE-SU-2015:2247](https://www.suse.com/support/update/patches/view.php?id=suse-su-2247)

Adobe Flash Player Multiple Bugs Let Remote
Users Bypass Security Controls and Execute
Arbitrary Code on the Target System -
SecurityTracker

www.securitytracker.com
text/html

 SECTRAK 1034318

[security-announce] openSUSE-SU-2015:2239-
1: important: Security update

lists.opensuse.org
text/html

 SUSE [openSUSE-SU-2015:2239](https://www.opensuse.org/support/update/patches/view.php?id=openSUSE-su-2239)

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	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	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	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: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:*****:						
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→