

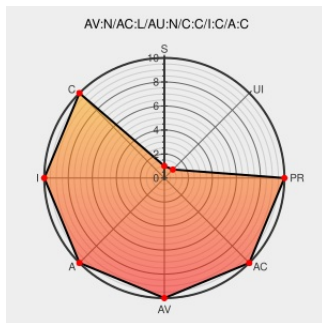


CVE-2015-8457

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

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

CVE-2015-8457

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

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

Stack-based buffer overflow in 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 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8407.

CVE-2015-8457 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](https://h20566.www2.hpe.com/text/html)
text/html

CONFIRM
h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05356388

Malformed Request

[cve.report \(archive\)](#)
text/html

BID 78802

Document Display | HPE Support Center

[h20566.www2.hpe.com](https://h20566.www2.hpe.com/text/html)
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
text/html

CONFIRM helpx.adobe.com/security/products/flash-player/apsb15-32.html

ZDI-15-636 Zero Day Initiative	www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-15-636
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
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	 SECTrack 1034318

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

System						
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→](#)

© [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](#)