



CVE-2015-7658

Published on: 11/11/2015 12:00:00 AM UTC

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

CVE-2015-7658

[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 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionInstanceOf arguments, a different vulnerability than CVE-2015-7651, CVE-2015-

7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.

CVE-2015-7658 has been assigned by psirt@adobe.com to track the vulnerability

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
Adobe Flash Player and AIR APSB15-28 Multiple Use After Free Remote Code Execution Vulnerabilities	cve.report (archive) text/html	🌐 BID 77533
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	CONFIRM helpx.adobe.com/security/products/flash-player/apsb15-28.html
ZDI-15-562 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-15-562

Adobe Flash Player Multiple Bugs Let Remote Users Write Data and Execute Arbitrary Code on the Target System - SecurityTracker

[www.securitytracker.com](http://www.securitytracker.com/text/html)
text/html

 **SECTRAK 1034111**

openSUSE-SU-2015:1984-1: moderate: Security update for flash-player

[lists.opensuse.org](https://lists.opensuse.org/text/html)
text/html

 **SUSE openSUSE-SU-2015:1984**

Red Hat Customer Portal

[web.archive.org](http://web.archive.org/text/html)
text/html
Inactive Link Not Archived

 **REDHAT RHSA-2015:2023**

Adobe Flash Player: Multiple vulnerabilities (GLSA 201511-02) — Gentoo Security

[security.gentoo.org](http://security.gentoo.org/text/html)
text/html

 **GENTOO GLSA-201511-02**

Red Hat Customer Portal

[web.archive.org](http://web.archive.org/text/html)
text/html
Inactive Link Not Archived

 **REDHAT RHSA-2015:2024**

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	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	19.0.0.185	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	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

Operating System	Apple	Mac Os X	-	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_&_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:19.0.0.185:*****:						
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:*****:						
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](#)