



CVE-2016-1018

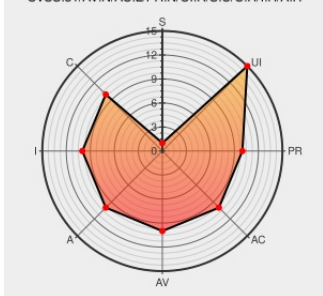
Published on: 04/08/2016 12:00:00 AM UTC

Last Modified on: 01/30/2023 06:15:00 PM UTC

CVE-2016-1018

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-XR data.

CVE-2016-1018 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
Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-16-228/
[security-announce] openSUSE-SU-2016:1306-1: important:	lists.opensuse.org	SUSE openSUSE-SU-2016:1306

Security update	text/html	
Microsoft Security Bulletin MS16-050 - Critical Microsoft Docs	docs.microsoft.com text/html	 MS MS16-050
Adobe Flash Player Multiple Bugs Lets Remote Users Execute Arbitrary Code and Bypass Security Restrictions - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1035509
[security-announce] SUSE-SU-2016:1305-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:1305
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	 CONFIRM helpx.adobe.com/security/products/flash-player/apsb16-10.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0610
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 Desktop Runtime	All	All	All	All
Application	Adobe	Air Sdk	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	20.0.0.286	All	All	All
Application	Adobe	Flash Player	20.0.0.306	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	20.0.0.286	All	All	All

Application	Adobe	Flash Player	20.0.0.200	All	All	All
Application	Adobe	Flash Player	20.0.0.306	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player Desktop Runtime	All	All	All	All
Operating System	Apple	Iphone Os	-	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Chrome Os	All	All	All	All
Operating System	Google	Chrome Os	-	All	All	All
Operating System	Google	Chrome Os	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	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
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows 10	All	All	All	All
Operating	Microsoft	Windows 10	-	All	All	All

System						
Operating System	Microsoft	Windows 10	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
cpe:2.3:a:adobe:air_desktop_runtime:*.***.***.***:						
cpe:2.3:a:adobe:air_sdk:*.***.***.***:						
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:20.0.0.286:*.***.***.***:						
cpe:2.3:a:adobe:flash_player:20.0.0.306:*.***.***.***:						
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:20.0.0.286:*.***.***.***:						
cpe:2.3:a:adobe:flash_player:20.0.0.306:*.***.***.***:						
cpe:2.3:a:adobe:flash_player:*.***.***.***:						
cpe:2.3:a:adobe:flash_player:*.***.***.***:esr:*.***:						
cpe:2.3:a:adobe:flash_player:*.***.***.***:chrome:*.***:						
cpe:2.3:a:adobe:flash_player:*.***.***.***:edge:*.***:						

cpe:2.3:a:adobe:flash_player:*****:internet_explorer:**:
cpe:2.3:a:adobe:flash_player:*****:
cpe:2.3:a:adobe:flash_player:*****:chrome:**:
cpe:2.3:a:adobe:flash_player:*****:edge:**:
cpe:2.3:a:adobe:flash_player:*****:internet_explorer:**:
cpe:2.3:a:adobe:flash_player_desktop_runtime:*****:
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:apple:mac_os_x:*****:
cpe:2.3:o:google:android:-*****:
cpe:2.3:o:google:chrome_os:*****:
cpe:2.3:o:google:chrome_os:-*****:
cpe:2.3:o:google:chrome_os:*****:
cpe:2.3:o:linux:linux_kernel:*****:
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:-*****:
cpe:2.3:o:microsoft:windows:*****:
cpe:2.3:o:microsoft:windows_10:*****:
cpe:2.3:o:microsoft:windows_10:-*****:
cpe:2.3:o:microsoft:windows_10:*****:
cpe:2.3:o:microsoft:windows_8.1:*****:
cpe:2.3:o:microsoft:windows_8.1:-*****:
cpe:2.3:o:microsoft:windows_8.1:*****:

No vendor comments have been submitted for this CVE

© [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](#)