



CVE-2014-0498

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0498
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-21 05:06:00 UTC
Updated	2018-12-13 15:54:00 UTC
Description	Stack-based buffer overflow in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Win

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Adobe Air	All	All	All	All
Application	Adobe	Adobe Air	All	All	All	All
Application	Adobe	Adobe Air Sdk	All	All	All	All
Application	Adobe	Adobe Air Sdk	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2014:0278-1: critical: flash-player: upd	SUSE	lists.opensuse.org	Mailing List, Third Party Advi
[security-announce] SUSE-SU-2014:0290-1: critical: Security update for f	SUSE	lists.opensuse.org	Mailing List, Third Party Advi

Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities	GENTOO	security.gentoo.org	Third Party Advisory
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Advisory
[security-announce] openSUSE-SU-2014:0277-1: critical: flash-player: upd	SUSE	lists.opensuse.org	Mailing List, Third Party Advisory
Adobe Security Bulletin	CONFIRM	helpx.adobe.com	Patch, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

Free CVE JSON API cve.report/api

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