



# CVE-2015-3043

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

## Summary

<b>CVE</b>	CVE-2015-3043
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@adobe.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-04-14 22:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202

## Risk And Classification

**EPSS:** 0.874240000 probability, percentile 0.994500000 (date 2026-04-02)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** NVD-CWE-noinfo

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Adobe
<b>Product</b>	Flash Player
<b>Name</b>	Adobe Flash Player Memory Corruption Vulnerability
<b>Required Action</b>	The impacted product is end-of-life and should be disconnected if still in use.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2015-3043">https://nvd.nist.gov/vuln/detail/CVE-2015-3043</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	14.0.0.125	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	14.0.0.145	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	14.0.0.176	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	14.0.0.179	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	15.0.0.152	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	15.0.0.167	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	15.0.0.189	All	All	All
Application	<a href="#">Adobe</a>	<a href="#">Flash Player</a>	15.0.0.223	All	All	All

Application	Adobe	Flash Player	15.0.0.239	All	All	All
Application	Adobe	Flash Player	15.0.0.246	All	All	All
Application	Adobe	Flash Player	16.0.0.235	All	All	All
Application	Adobe	Flash Player	16.0.0.257	All	All	All
Application	Adobe	Flash Player	16.0.0.287	All	All	All
Application	Adobe	Flash Player	16.0.0.296	All	All	All
Application	Adobe	Flash Player	17.0.0.134	All	All	All
Application	Adobe	Flash Player	14.0.0.125	All	All	All
Application	Adobe	Flash Player	14.0.0.145	All	All	All
Application	Adobe	Flash Player	14.0.0.176	All	All	All
Application	Adobe	Flash Player	14.0.0.179	All	All	All
Application	Adobe	Flash Player	15.0.0.152	All	All	All
Application	Adobe	Flash Player	15.0.0.167	All	All	All
Application	Adobe	Flash Player	15.0.0.189	All	All	All
Application	Adobe	Flash Player	15.0.0.223	All	All	All
Application	Adobe	Flash Player	15.0.0.239	All	All	All
Application	Adobe	Flash Player	15.0.0.246	All	All	All
Application	Adobe	Flash Player	16.0.0.235	All	All	All
Application	Adobe	Flash Player	16.0.0.257	All	All	All
Application	Adobe	Flash Player	16.0.0.287	All	All	All
Application	Adobe	Flash Player	16.0.0.296	All	All	All
Application	Adobe	Flash Player	17.0.0.134	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
Operating System	Apple	Mac Os X	-	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
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	All	All	All

Operating System	<a href="#">Novell</a>	<a href="#">Suse Linux Enterprise Workstation Extension</a>	12.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Supplementary</a>	5.0	client	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Supplementary</a>	5.0	client	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary Eus</a>	6.6.z	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Supplementary Eus</a>	6.6.z	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Supplementary</a>	5.0	server	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Supplementary</a>	5.0	server	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation Supplementary</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation Supplementary</a>	6.0	All	All	All

## References

### Reference

[Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow - Exploits Database](#)

[Red Hat Customer Portal](#)

[Adobe Flash Player Multiple Unspecified Memory Corruption Vulnerabilities](#)

[\[security-announce\] openSUSE-SU-2015:0725-1: important: Security update](#)

[\[security-announce\] openSUSE-SU-2015:0718-1: important: Security update](#)

[Adobe Flash Player: Multiple vulnerabilities \(GLSA 201504-07\) — Gentoo security](#)

[\[security-announce\] SUSE-SU-2015:0723-1: important: Security update for](#)

[Adobe Security Bulletin](#)

[\[security-announce\] SUSE-SU-2015:0722-1: important: Security update for](#)

[Adobe Flash Player Multiple Bugs Let Remote Users Bypass ASLR, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - Se](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)

No vendor comments have been submitted for this CVE.

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

© [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](#) 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](#)**