



# CVE-2016-7876

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

## Summary

<b>CVE</b>	CVE-2016-7876
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@adobe.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-15 06:59:00 UTC
<b>Updated</b>	2022-11-16 21:31:00 UTC
<b>Description</b>	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulne

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	23.0.0.207	All	All	All
Application	Adobe	Flash Player	23.0.0.207	All	All	All
Application	Adobe	Flash Player	23.0.0.207	All	All	All
Application	Adobe	Flash Player	23.0.0.207	All	All	All
Application	Adobe	Flash Player	23.0.0.207	All	All	All
Application	Adobe	Flash Player	23.0.0.207	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
Application	Adobe	Flash Player For Linux	All	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	Chrome Os	All	All	All	All

Operating System	<a href="#">Google</a>	<a href="#">Chrome Os</a>	-	All	All	All
Operating System	<a href="#">Google</a>	<a href="#">Chrome Os</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 8.1</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 8.1</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 8.1</a>	All	All	All	All

## References

Reference	Source
Adobe Flash Player: Multiple vulnerabilities (GLSA 201701-17) — Gentoo security	GENTOO
[security-announce] SUSE-SU-2016:3148-1: critical: Security update for f	SUSE
Adobe Security Bulletin	CONFIRM
Red Hat Customer Portal	REDHAT
Adobe Flash Player APSB16-39 Multiple Unspecified Memory Corruption Vulnerabilities	BID
Microsoft Security Bulletin MS16-154 - Critical   Microsoft Docs	MS
Adobe Flash Player Multiple Bugs Let Remote Users Bypass Security Restrictions and Execute Arbitrary Code - SecurityTracker	SECTRAC
openSUSE-SU-2016:3160-1: moderate: Security update for flash-player	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710422](#) Gentoo Linux Adobe Flash Player Multiple Vulnerabilities (GLSA 201701-17)

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)