



CVE-2016-4225

Published on: 07/12/2016 12:00:00 AM UTC

Last Modified on: 01/26/2023 01:53:00 PM UTC

CVE-2016-4225

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Flash Player](#) from [Adobe](#) contain the following vulnerability:

Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4224.

CVE-2016-4225 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: **6.8 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Adobe Flash Player APSB16-25 Type Confusion Multiple Remote Code Execution Vulnerabilities

[cve.report \(archive\)](#)
[text/html](#)

[BID 91718](#)

[security-announce] openSUSE-SU-2016-1802-1: important

[lists.opensuse.org](#)

[SUSE openSUSE-SU-2016-1802](#)

[security-announce] openSUSE-OS-2016:1826-1: important: Security update	lists.opensuse.org text/html	 openSUSE-OS-2016:1826
[security-announce] SUSE-SU-2016:1826-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:1826
Adobe Flash Player Multiple Bugs Lets Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	 SECTRACK 1036280
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2016:1423
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	 CONFIRM helpx.adobe.com/security/products/flash-player/apsb16-25.html
Adobe Flash Player: Multiple vulnerabilities (GLSA 201607-03) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201607-03
Microsoft Security Bulletin MS16-093 - Critical Microsoft Docs	docs.microsoft.com text/html	 MS MS16-093
Zero Day Initiative	www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-16-427
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	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	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	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 System	Microsoft	Windows 10	-	All	All	All
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:flash_player:*****:						
cpe:2.3:a:adobe:flash_player:*****:esr:****:						
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:mac_os_x:*****:						
cpe:2.3:o:apple:mac_os_x:-:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
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

[← 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