



CVE-2016-4286

Published on: 10/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:58 PM UTC

CVE-2016-4286

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

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

Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.

CVE-2016-4286 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
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	CONFIRM helpx.adobe.com/security/products/flash-player/psb16-32.html

Adobe Flash Player Multiple Flaws Let Remote Users Bypass Security Restrictions and Execute Arbitrary Code - SecurityTracker

Third Party Advisory
VDB Entry
www.securitytracker.com
text/html

SECTrack 1036985

Adobe Flash Player: Multiple vulnerabilities (GLSA 201610-10) — Gentoo security

Third Party Advisory
security.gentoo.org
text/html

Gentoo GLSA-201610-10

Red Hat Customer Portal

Third Party Advisory
web.archive.org
text/html
Inactive Link Not Archived

Redhat RHSA-2016:2057

Adobe Flash Player CVE-2016-4286 Unspecified Security Bypass Vulnerability

Third Party Advisory
VDB Entry
cve.report (archive)
text/html

BID 93497

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 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	All
Operating System	Google	Chrome Os	All	All	All	All
Operating System	Google	Chrome Os	All	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	All
Operating System	Microsoft	Windows	All	All	All	All

	Operating System	Microsoft	Windows 10	-	All	All	All
	Operating System	Microsoft	Windows 10	-	All	All	All
	Operating System	Microsoft	Windows 8.1	-	All	All	All
	Operating System	Microsoft	Windows 8.1	-	All	All	All
	Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
	Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
	Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
	Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
	Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
	Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
	Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
	cpe:2.3:a:adobe:flash_player:*:*:*:*:linux:*:*:						
	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_desktop_runtime:*:*:*:*:*:						
	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: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_10:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:0:microsoft:windows_8.1:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0.*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:5.0.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0.*:*:*:*:*.*.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)