



CVE-2016-4143

Published on: 06/16/2016 12:00:00 AM UTC

Last Modified on: 11/19/2021 11:14:00 AM UTC

CVE-2016-4143

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

CVE-2016-4143 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
[security-announce] openSUSE-SU-2016:1625-1: critical: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1625
Microsoft Security Bulletin MS16-083 - Critical Microsoft Docs	docs.microsoft.com text/html	MS MS16-083

[security-announce] openSUSE-SU-2016:1621-1: critical: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1621
[security-announce] SUSE-SU-2016:1613-1: critical: Security update for f	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:1613
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	 CONFIRM helpx.adobe.com/security/products/flash-player/apsb16-18.html
Adobe Flash Player Multiple Flaws Let Remote Users Execute Arbitrary Code, Bypass Same Origin Policy, and Obtain Potentially Sensitive Information - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1036117
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2016:1238
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
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	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	Macos	All	All	All	All
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	All	All	All	All
Operating System	Apple	Mac Os	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
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	1511	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
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	r2	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	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
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	-	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	sp1	All	All
cpe:2.3:a:adobe:flash_player:-:*:*:*:*:*:						
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:*:*:*:*:internet_explorer_11:*:*:						
cpe:2.3:a:adobe:flash_player_desktop_runtime:*:*:*:*:*:*:						
cpe:2.3:a:adobe:flash_player_for_linux:*:*:*:*:*:*:						

Spencer, William; _praj_ v. _re_ munda . . .

```
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os:*:*:*:*:*:*:
```

```
cpe:2.3:o:apple:mac_os:*.:.:.:.:.:.:.:
```

```
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_10:1511:*:*:*:*:*:
```

```
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:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows rt 8.1:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*
```

```
cpe:2.3:o:microsoft:windows_server_2012:-r2:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:
```

```
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:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:12:sp1:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_workstation_extension:12:-:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_workstation_extension:12:sp1:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)