



CVE-2015-7648

Published on: 10/18/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7648

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

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

Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7647.

CVE-2015-7648 has been assigned by psirt@adobe.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Adobe Security Bulletin

Tags

[Patch](#)
[Vendor Advisory](#)
[helpx.adobe.com](#)
[text/html](#)

Link

CONFIRM
helpx.adobe.com/security/products/flash-player/apsb15-27.html

Adobe Flash Player Type Confusion Errors Let Remote Users Execute Arbitrary Code - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

SECTRAK 1033850

Red Hat Customer Portal

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

REDHAT RHSA-2015:1913

Adobe Flash Player CVE-2015-7648 Unspecified Remote Code Execution Vulnerability

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

BID 77116

Adobe Flash - Type Confusion in Serialization with ObjectEncoder.dynamicPropertyWriter - Multiple dos Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)

EXPLOIT-DB 38970

 GENTOO GLSA-201511-02

Adobe Flash Player: Multiple vulnerabilities (GLSA 201511-02) — Gentoo Security

Red Hat Customer Portal

web.archive.org

text/html

Inactive Link

Not Archived

 REDHAT RHSA-2015:2024

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
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

```
cpe:2.3:a:adobe:flash_player:*.:*:*:*:*:*:*:
```

```
cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:
```

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

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

```
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:-:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

© [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](#)