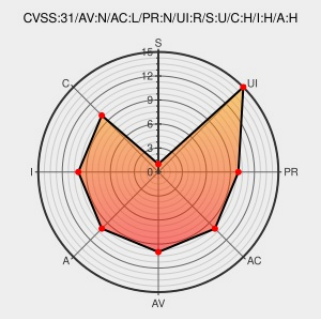
CVE-2017-11292

Published on: 10/21/2017 12:00:00 AM UTC

Last Modified on: 01/27/2023 07:24:00 PM UTC

CVE-2017-11292

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Flash Player from Adobe contain the following vulnerability:

Adobe Flash Player version 27.0.0.159 and earlier has a flawed bytecode verification procedure, which allows for an untrusted value to be used in the calculation of an array index. This can lead to type confusion, and successful exploitation could lead to arbitrary code execution.

CVE-2017-11292 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 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Adobe Flash Player Type Confusion Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTRACK 1039582

	text/html	
Adobe Security Bulletin	Issue Tracking Vendor Advisory helpx.adobe.com text/html	CONFIRM helpx.adobe.com/security/products/flash-player/apsb17-32.html
Adobe Flash Player CVE-2017-11292 Type Confusion Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 101286
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2017:2899
Adobe Flash Player: Remote execution of arbitrary code (GLSA 201710-22) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201710-22

Related QID Numbers

710552 Gentoo Linux Adobe Flash Player Remote execution of arbitrary code Vulnerability (GLSA 201710-22)

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	Macos	All	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
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
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

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:*:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:flash_player:*:*:*:*:*:chrome:*:*:

cpe:2.3:a:adobe:flash_player_desktop_runtime:*:*:*:*:*:*:*:*:

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: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:*:*:*:*:*:*:*:*:

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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