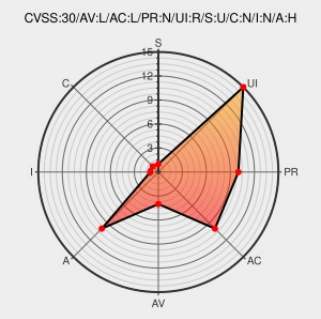
CVE-2017-16794

Published on: 11/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:38 PM UTC

CVE-2017-16794

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



Certain versions of Swftools from Swftools contain the following vulnerability:

The png_load function in lib/png.c in SWFTools 0.9.2 does not properly validate a multiplication of width and bits-per-pixel values, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file, as demonstrated by an erroneous png_load call that occurs because of incorrect integer data types in png2swf.

CVE-2017-16794 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
A heapoverflow bug of png2swf. · Issue #50 · matthiaskramm/swftools · GitHub	Issue Tracking, Third Party Advisory	MISC github.com/matthiaskramm/swftools/issues/50

github.com
text/html

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	Swftools	Swftools	0.9.2	All	All	All
Application	Swftools	Swftools	0.9.2	All	All	All

cpe:2.3:a:swftools:swftools:0.9.2:*:*:*:*:*:*:*

cpe:2.3:a:swftools:swftools:0.9.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→