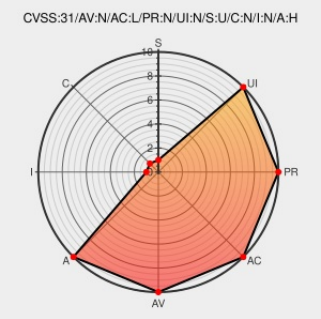
CVE-2017-6960

Published on: 03/17/2017 12:00:00 AM UTC

Last Modified on: 01/20/2023 03:03:00 PM UTC

CVE-2017-6960

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



Certain versions of Apng2gif from Apng2gif Project contain the following vulnerability:

An issue was discovered in apng2gif 1.7. There is an integer overflow resulting in a heap-based buffer over-read, related to the load_apng function and the imagesize variable.

CVE-2017-6960 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
#854367 - apng2gif: CVE-2017-6960: Integer overflow resulting in heap buffer overflow - Debian Bug report logs	Issue Tracking, Third Party Advisory, bugs.debian.org, text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=854367

USN-4513-1: apng2gif vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4513-1
[SECURITY] [DLA 2165-1] apng2gif security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200331 [SECURITY] [DLA 2165-1] apng2gif security update

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.

Related QID Numbers

179055 Debian Security Update for apng2gif (DLA 2911-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apng2gif Project	Apng2gif	1.7	All	All	All
Application	Apng2gif Project	Apng2gif	1.7	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All

cpe:2.3:a:apng2gif_project:apng2gif:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:apng2gif_project:apng2gif:1.7:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→