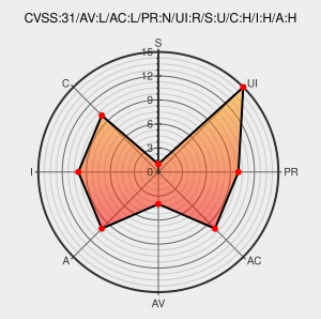
CVE-2021-45910

Published on: Not Yet Published

Last Modified on: 03/24/2022 03:52:00 PM UTC

CVE-2021-45910

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow within the main function. It allows an attacker to write data outside of the allocated buffer. The attacker has control over a part of the address that data is written to, control over the written data, and (to some extent) control over the amount of data that is written.

CVE-2021-45910 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
#1002667 - gif2apng: Heap based buffer overflow in the main function - Debian Bug report logs	bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=1002667
[SECURITY] [DLA 2937-1] gif2apng security update	lists.debian.org	MLIST [debian-lts-announce] 20220307 [SECURITY]

[SECURITY] [DLA 2937-1] gif2apng security update — lists.debian.org — text/html — [DLA 2937-1] gif2apng 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

179105 Debian Security Update for gif2apng (DLA 2937-1)

181029 Debian Security Update for gif2apng (CVE-2021-45910)

199252 Ubuntu Security Notification for gif2apng Vulnerabilities (USN-5969-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gif2apng Project	Gif2apng	1.9	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:gif2apng_project:gif2apng:1.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-45910 Description: An issue was discovered in gif2apng 1.9. There is a… twitter.com/i/web/status/1…	2021-12-28 00:56:12
@CVEreport	CVE-2021-45910 : An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow within the main fun… twitter.com/i/web/status/1…	2021-12-28 01:06:44

← Previous ID Next ID→