



CVE-2021-45911

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-45911
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-28 01:15:00 UTC
Updated	2022-03-24 15:53:00 UTC
Description	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow in the main function. It allows an attacker to

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
#1002687 - gif2apng: Heap based buffer overflow in processing of delays in the main function - Debian Bug report logs	MISC	bugs.d
[SECURITY] [DLA 2937-1] gif2apng security update	MLIST	lists.de
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [179105](#) Debian Security Update for gif2apng (DLA 2937-1)
- [181020](#) Debian Security Update for gif2apng (CVE-2021-45911)
- [199252](#) Ubuntu Security Notification for gif2apng Vulnerabilities (USN-5969-1)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)