



CVE-2022-47517

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-47517
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-18 05:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	An issue was discovered in the libsofia-sip fork in drachtio-server before 0.8.19. It allows remote attackers to cause a denial of service (CPU consumption) via crafted SIP messages.

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drachtio	Drachtio-server	All	All	All	All

References

Reference	Source	Link
heap-based buffer overflow in (url_canonize2 libsofia-sip-ua/url/url.c ?) - Issue #243 · drachtio/drachtio-server · GitHub	MISC	github.com
better fix for prev commit · davehorton/sofia-sip@bfc79d8 · GitHub	MISC	github.com
fix off-by-one access triggered eg by Contact: % · davehorton/sofia-sip@22c1bd1 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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