



CVE-2022-45909

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

Summary

CVE	CVE-2022-45909
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-26 03:15:00 UTC
Updated	2023-02-01 15:26:00 UTC
Description	drachtio-server before 0.8.19 has a heap-based buffer over-read via a long Request-URI in an INVITE request.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drachtio	Drachtio-server	All	All	All	All
Application	Drachtio	Drachtio-server	0.8.18	-	All	All

References

Reference

- sending an invite with a request-uri longer than 255 characters can c... · drachtio/drachtio-server@a63d018 · GitHub
- sending an invite with a request-uri longer than 255 characters can c... by davehorton · Pull Request #238 · drachtio/drachtio-server · GitHub
- Comparing v0.8.18...v0.8.19 · drachtio/drachtio-server · GitHub
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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