



# CVE-2022-45474

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-45474
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-18 18:15:00 UTC
<b>Updated</b>	2022-11-28 22:12:00 UTC
<b>Description</b>	drachtio-server 0.8.18 has a request-handler.cpp event_cb use-after-free for any request.

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Drachtio</a>	<a href="#">Drachtio-server</a>	0.8.18	All	All	All

## References

Reference	Source	Link
Use-after-free in event_cb when drachtio-server receives a call · Issue #240 · drachtio/drachtio-server · GitHub	MISC	<a href="#">github.com</a>
fix for use-after-free (#240) · drachtio/drachtio-server@860f025 · GitHub	CONFIRM	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)