



CVE-2022-23492

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

Summary

CVE	CVE-2022-23492
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-08 01:15:00 UTC
Updated	2023-07-14 19:22:00 UTC
Description	go-libp2p is the official libp2p implementation in the Go programming language. Version `0.18.0` and older of go-libp2p are v

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Protocol	Libp2p	All	All	All	All

References

Reference	Source	Link	Tags
libp2p DoS vulnerability from lack of resource management · Advisory · libp2p/go-libp2p · GitHub	MISC	github.com	
Merge pull request #1275 from libp2p/rcmgr · libp2p/go-libp2p@15d7dfb · GitHub	MISC	github.com	
DOS Mitigation :: libp2p Documentation	MISC	docs.libp2p.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

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