



CVE-2023-39533

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

Summary

CVE	CVE-2023-39533
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-08 19:15:00 UTC
Updated	2023-10-31 19:08:00 UTC
Description	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious pe

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All
Application	Libp2p	Go-libp2p	All	All	All	All
Application	Libp2p	Go-libp2p	0.29.0	All	All	All
Application	Quic Project	Quic	All	All	All	All

References

Reference	Source
core/crypto: restrict RSA keys to <= 8192 bits (#2454) · libp2p/go-libp2p@0cce607 · GitHub	MISC
core/crypto: restrict RSA keys to <= 8192 bits by MarcoPolo · Pull Request #2454 · libp2p/go-libp2p · GitHub	MISC
update qtls to restrict RSA keys in certificates to <= 8192 bits by marten-seemann · Pull Request #4012 · quic-go/quic-go · GitHub	MISC
crypto/tls: verifying certificate chains containing large RSA keys is slow [CVE-2023-29409] · Issue #61460 · golang/go · GitHub	MISC
libp2p nodes vulnerable to attack using large RSA keys · Advisory · libp2p/go-libp2p · GitHub	MISC
core/crypto: restrict RSA keys to <= 8192 bits (#2454) · libp2p/go-libp2p@445be52 · GitHub	MISC
crypto/tls: restrict RSA keys in certificates to <= 8192 bits · golang/go@2350afd · GitHub	MISC
core/crypto: restrict RSA keys to <= 8192 bits (#2454) · libp2p/go-libp2p@e30fcf7 · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[907821](#) Common Base Linux Mariner (CBL-Mariner) Security Update for golang (27872-2)

[994783](#) GO (Go) Security Update for github.com/libp2p/go-libp2p (GHSA-876p-8259-xjgg)

© [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](#)