



CVE-2023-46239

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

Summary

CVE	CVE-2023-46239
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-31 16:15:00 UTC
Updated	2023-11-09 00:14:00 UTC
Description	quic-go is an implementation of the QUIC protocol in Go. Starting in version 0.37.0 and prior to version 0.37.3, by serializing

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quic-go Project	Quic-go	All	All	All	All

References

Reference	Source
Release v0.37.3 · quic-go/quic-go · GitHub	M
fix handling of ACK frames serialized after CRYPTO frames (#4018) · quic-go/quic-go@b6a4725 · GitHub	M
remote-triggered panic due to unexpected frame serialization order when completing the handshake · Advisory · quic-go/quic-go · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[995769](#) GO (Go) Security Update for github.com/quic-go/quic-go (GHSA-3q6m-v84f-6p9h)

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