



CVE-2022-24759

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

Summary

CVE	CVE-2022-24759
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-17 17:15:00 UTC
Updated	2022-03-23 19:01:00 UTC
Description	`@chainsafe/libp2p-noise` contains TypeScript implementation of noise protocol, an encryption protocol used in libp2p. `@c

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chainsafe	Js-libp2p-noise	All	All	All	All

References

Reference	Source	Link	Tags
Failure to validate signature during handshake · Advisory · ChainSafe/js-libp2p-noise · GitHub	CONFIRM	github.com	
Release Release v5.0.3 · ChainSafe/js-libp2p-noise · GitHub	MISC	github.com	
chore: Fix signature validation bug by mpetrunic · Pull Request #130 · ChainSafe/js-libp2p-noise · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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