



CVE-2022-39389

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

Summary

CVE	CVE-2022-39389
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-17 22:15:00 UTC
Updated	2022-11-22 16:49:00 UTC
Description	Lightning Network Daemon (Ind) is an implementation of a lightning bitcoin overlay network node. All Ind nodes before versi

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Btcd Project	Btcd	All	All	All	All
Application	Lightning Network Daemon Project	Lightning Network Daemon	All	All	All	All

References

Reference
Release Ind v0.15.4-beta · lightningnetwork/Ind · GitHub
mod+build: bump btcd version to v0.23.3 and bump Ind version to v0.15.4-beta by guggero · Pull Request #7098 · lightningnetwork/Ind · GitHub
[bug]: CRITICAL! Unable to process chain reorg / too many witness items to fit into max message size · Issue #7096 · lightningnetwork/Ind · GitHub
Witness Block Parsing DoS Vulnerability · Advisory · lightningnetwork/Ind · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#)