



CVE-2020-11093

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-11093
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-24 20:15:00 UTC
Updated	2020-12-31 19:25:00 UTC
Description	Hyperledger Indy Node is the server portion of a distributed ledger purpose-built for decentralized identity. In Hyperledger Ir

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Indy-node	All	All	All	All
Application	Linuxfoundation	Indy-node	All	All	All	All

References

Reference

changed auth rules check to skip those without verkey and role · hyperledger/indy-node@55056f2 · GitHub

indy-node/CHANGELOG.md at master · hyperledger/indy-node · GitHub

Updating a DID with a nym transaction will be written to the ledger if neither ROLE or VERKEY are being changed, regardless of sender. · Adv

indy-node/auth_rules.md at master · hyperledger/indy-node · 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)