# CVE-2020-11093

MITRE | NVD | CVE.ORG | Print: PDF

## 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.