CVE-2022-24772

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-24772
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-18 14:15:00 UTC
Updated	2022-03-28 14:10:00 UTC
Description	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0,

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digitalbazaar	Forge	All	All	All	All

References

Reference
Fix signature verification issues. · digitalbazaar/forge@3f0b49a · GitHub
Add advisory links. · digitalbazaar/forge@bb822c0 · GitHub
RSA PKCS#1 v1.5 signature verification failing to check tailing garbage bytes can lead to signature forgery. · Advisory · digitalbazaar/forge · G
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180870 Debian Security Update for node-node-forge (CVE-2022-24772)

CVE.report and Source URL Uptime Status status.cve.report