



CVE-2022-24772

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

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 trailing 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)

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](#)