



# CVE-2022-24773

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

## Summary

<b>CVE</b>	CVE-2022-24773
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-18 14:15:00 UTC
<b>Updated</b>	2022-03-28 14:20:00 UTC
<b>Description</b>	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	Source	Li
Fix signature verification issues. · digitalbazaar/forge@3f0b49a · GitHub	MISC	<a href="#">git</a>
Add advisory links. · digitalbazaar/forge@bb822c0 · GitHub	MISC	<a href="#">git</a>
RSA PKCS#1 v1.5 signature verification leniency in checking `DigestInfo` structure. · Advisory · digitalbazaar/forge · GitHub	CONFIRM	<a href="#">git</a>
CVE Program record	CVE.ORG	<a href="#">wv</a>
NVD vulnerability detail	NVD	<a href="#">nv</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[180862](#) Debian Security Update for node-node-forge (CVE-2022-24773)

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](#)**