



CVE-2021-29444

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

Summary

CVE	CVE-2021-29444
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-16 22:15:00 UTC
Updated	2023-03-21 13:18:00 UTC
Description	jose-browser-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jose-node-cjs-runtime Project	Jose-node-cjs-runtime	All	All	All	All
Application	Jose Project	Jose	All	All	All	All

References

Reference	Source	Link
Padding Oracle Attack due to Observable Timing Discrepancy in jose-browser-runtime · Advisory · panva/jose · GitHub	CONFIRM	github.
jose-browser-runtime - npm	MISC	www.n
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982738](#) Nodejs (npm) Security Update for jose-browser-runtime (GHSA-94hh-pjjg-rwmr)

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](#).

Free CVE JSON API cve.report/api

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