



CVE-2021-29443

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

Summary

CVE	CVE-2021-29443
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-16 18:15:00 UTC
Updated	2021-04-23 20:38:00 UTC
Description	jose is an npm library providing a number of cryptographic operations. In vulnerable versions AES_CBC_HMAC_SHA2 Alg

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jose Project	Jose	All	All	All	All

References

Reference	Source	Link	Tags
jose - npm	MISC	www.npmjs.com	
Padding Oracle Attack due to Observable Timing Discrepancy in jose · Advisory · panva/jose · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982742](#) Nodejs (npm) Security Update for jose (GHSA-58f5-hfqc-jgch)

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