CVE-2022-25901

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-25901
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-18 05:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	Versions of the package cookiejar before 2.1.4 are vulnerable to Regular Expression Denial of Service (ReDoS) via the Coo

Risk And Classification

Problem Types: CWE-1333

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
fix: add a guard against maliciously-sized cookies by andyburke · Pull Request #39 · bmeck/node-cookiejar · GitHub	MISC	github.cor
fix: add a guard against maliciously-sized cookies by andyburke · Pull Request #39 · bmeck/node-cookiejar · GitHub	MISC	github.cor
[SECURITY] [DLA 3561-1] node-cookiejar security update	MISC	lists.debia
github.com/bmeck/node-cookiejar/blob/master/cookiejar.js%23L73	MISC	github.cor
Regular Expression Denial of Service (ReDoS) in cookiejar | CVE-2022-25901 | Snyk	MISC	security.s
Regular Expression Denial of Service (ReDoS) in org.webjars.npm:cookiejar | CVE-2022-25901 | Snyk	MISC	security.s
node-cookiejar/cookiejar.js at master · bmeck/node-cookiejar · GitHub	MITRE	github.cor
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183822 Debian Security Update for node-cookiejar (CVE-2022-25901)

6000158 Debian Security Update for node-cookiejar (DLA 3561-1)

Free CVE JSON API cve.report/api

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