



CVE-2022-21803

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

Summary

CVE	CVE-2022-21803
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-12 16:15:00 UTC
Updated	2022-04-20 14:07:00 UTC
Description	This affects the package nconf before 0.11.4. When using the memory engine, it is possible to store a nested JSON repres

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Prototype Pollution in org.webjars.npm:nconf CVE-2022-21803 Snyk	MISC	snyk.io
Prototype Pollution in nconf CVE-2022-21803 Snyk	MISC	snyk.io
fix(security): prevent prototype pollution in memory store by mhamann · Pull Request #397 · indexzero/nconf · GitHub	MISC	github.co
Release v0.11.4 · indexzero/nconf · GitHub	MISC	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

LEGACY: Alessio Della Libera of Snyk Research Team

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)