



CVE-2022-21721

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

Summary

CVE	CVE-2022-21721
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-28 22:15:00 UTC
Updated	2023-07-24 13:52:00 UTC
Description	Next.js is a React framework. Starting with version 12.0.0 and prior to version 12.0.9, vulnerable code could allow a bad act

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vercel	Next.js	All	All	All	All

References

Reference	Source	Link	Tags
Release v12.0.9 · vercel/next.js · GitHub	MISC	github.com	
Fix static file check with i18n by ijkk · Pull Request #33503 · vercel/next.js · GitHub	MISC	github.com	
DOS Vulnerability for self-hosted next.js apps using i18n · Advisory · vercel/next.js · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)