CVE-2022-24824

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-24824
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-14 22:15:00 UTC
Updated	2022-04-22 19:53:00 UTC
Description	Discourse is an open source platform for community discussion. In affected versions an attacker can poison the cache for a

Risk And Classification

Problem Types: CWE-829

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Discourse	Discourse	All	All	All	All
Application	Discourse	Discourse	2.9.0	beta1	All	All
Application	Discourse	Discourse	2.9.0	beta2	All	All
Application	Discourse	Discourse	2.9.0	beta3	All	All

References

Reference	Source	Link
SECURITY: Ensure user-agent-based responses are cached separately (st… · discourse/discourse@b72b0da · GitHub	MISC	github
Anonymous user cache poisoning via maliciously formed request · Advisory · discourse/discourse · GitHub	CONFIRM	github
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

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