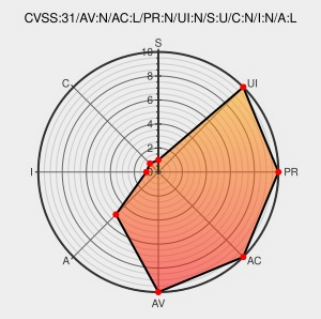
CVE-2022-31182

Published on: Not Yet Published

Last Modified on: 08/08/2022 03:22:00 PM UTC

CVE-2022-31182 - advisory for GHSA-4ff8-3j78-w6pp

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Discourse from Discourse contain the following vulnerability:

Discourse is the an open source discussion platform. In affected versions a maliciously crafted request for static assets could cause error responses to be cached by Discourse's default NGINX proxy configuration. A corrected NGINX configuration is included in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVE-2022-31182 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **< 2.8.7**

Affected Vendor/Software: **discourse** - **discourse** version **< 2.9.0.beta8**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	LOW

CVE References

Description	Tags	Link
Cache poisoning via maliciously-formed request · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-4ff8-3j78-w6pp
SECURITY: Do not cache error responses for static assets (stable) · discourse/discourse@7af2554 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/7af25544c3940c4d046c51f4cfac9c72a06d4f50

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Discourse	Discourse	All	All	All	All
Application	Discourse	Discourse	2.9.0	beta7	All	All

cpe:2.3:a:discourse:discourse:*:*:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta7:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31182 : Discourse is the an open source discussion platform. In affected versions a maliciously crafted re… twitter.com/i/web/status/1…	2022-08-01 19:45:58
@LinInfoSec	Nginx - CVE-2022-31182: github.com/discourse/disc…	2022-08-01 23:01:41
/r/netcve	CVE-2022-31182	2022-08-01 20:38:19

← Previous ID

Next ID→