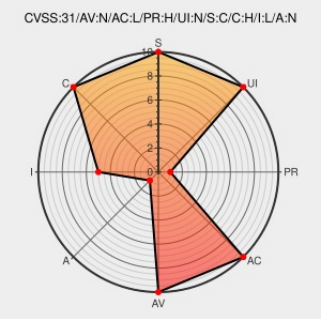
CVE-2022-39241

Published on: Not Yet Published

Last Modified on: 11/04/2022 03:37:00 PM UTC

CVE-2022-39241 - advisory for GHSA-rcc5-28r3-23rr

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



Certain versions of Discourse from Discourse contain the following vulnerability:

Discourse is a platform for community discussion. A malicious admin could use this vulnerability to perform port enumeration on the local host or other hosts on the internal network, as well as against hosts on the Internet. Latest `stable`, `beta`, and `test-passed` versions are now patched. As a workaround, self-hosters can use `DISCOURSE_BLOCKED_IP_BLOCKS` env var (which overrides `blocked_ip_blocks` setting) to stop webhooks from accessing private IPs.

CVE-2022-39241 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **<= 2.8.9**

Affected Vendor/Software: **discourse** - **discourse** version **<= 2.9.0.beta10**

CVSS3 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Insufficient Server Side Request Forgery protections · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-rcc5-28r3-23rr

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	beta1	All	All
Application	Discourse	Discourse	2.9.0	beta10	All	All
Application	Discourse	Discourse	2.9.0	beta2	All	All
Application	Discourse	Discourse	2.9.0	beta3	All	All
Application	Discourse	Discourse	2.9.0	beta4	All	All
Application	Discourse	Discourse	2.9.0	beta5	All	All
Application	Discourse	Discourse	2.9.0	beta6	All	All
Application	Discourse	Discourse	2.9.0	beta7	All	All
Application	Discourse	Discourse	2.9.0	beta8	All	All
Application	Discourse	Discourse	2.9.0	beta9	All	All

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

cpe:2.3:a:discourse:discourse:2.9.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta10:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta4:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta5:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta6:*:*:*:*:*:*:

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

cpe:2.3:a:discourse:discourse:2.9.0:beta8:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.9.0:beta9:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@CVEreport	CVE-2022-39241 : Discourse is a platform for community discussion. A malicious admin could use this vulnerability t… twitter.com/i/web/status/1…	2022-11-02 16:38:27
/r/netcve	CVE-2022-39241	2022-11-02 17:38:37

← Previous ID

Next ID→