



CVE-2022-39241

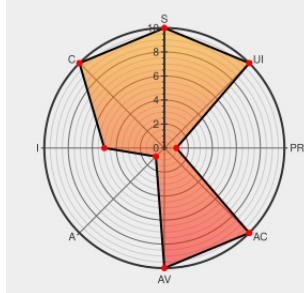
Published on: Not Yet Published

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](#)

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N



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

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	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 >](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)