

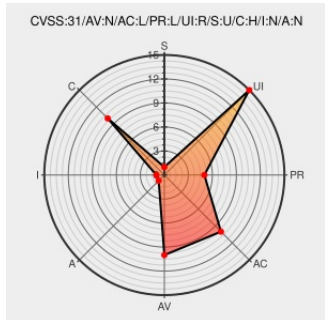


CVE-2022-31096

Published on: Not Yet Published

Last Modified on: 07/07/2022 04:31:00 PM UTC

CVE-2022-31096 - advisory for GHSA-rvp8-459h-282r

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Discourse](#) from [Discourse](#) contain the following vulnerability:

Discourse is an open source discussion platform. Under certain conditions, a logged in user can redeem an invite with an email that either doesn't match the invite's email or does not adhere to the email domain restriction of an invite link. The impact of this flaw is aggravated when the invite has been configured to add the user that accepts the invite into restricted groups. Once a user has been incorrectly added to a restricted group, the user may then be able to view content which that are restricted to the respective group. Users are advised to upgrade to the current stable releases. There are no known workarounds to this issue.

CVE-2022-31096 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [discourse](#) - **discourse** version < 2.8.5; **stable branch**

Affected Vendor/Software: [discourse](#) - **discourse** version < 2.9.0.beta6; **beta brach**

CVSS3 Score: **5.7 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality	Integrity	Availability

Impact	Impact	Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Invites restricted to an email or invite links restricted to an email domain may be bypassed by a under certain conditions · Advisory · discourse/discourse · GitHub	github.com text/html	 CONFIRM github.com/discourse/discourse/security/advisories/GHSA-rvp8-459h-282r
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	2.9.0	beta1	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	All	All	All	All

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

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:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31096 : Discourse is an open source discussion platform. Under certain conditions, a logged in user can re... twitter.com/i/web/status/1...	2022-06-27 21:45:03
 @threatmeter	CVE-2022-31096 Discourse is an open source discussion platform. Under certain conditions, a logged in user can rede... twitter.com/i/web/status/1...	2022-06-28 07:09:44

[← 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](#)