

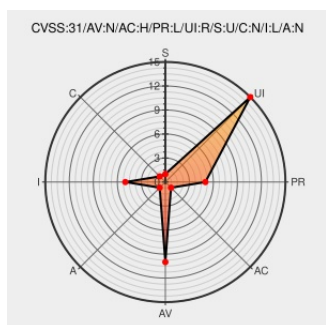


CVE-2022-31025

Published on: Not Yet Published

Last Modified on: 07/21/2023 05:09:00 PM UTC

CVE-2022-31025 - advisory for GHSA-x7jh-mx5q-6f9q

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

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

Discourse is an open source platform for community discussion. Prior to version 2.8.4 on the `stable` branch and 2.9.0beta5 on the `beta` and `tests-passed` branches, inviting users on sites that use single sign-on could bypass the `must\_approve\_users` check and invites by staff are always approved automatically. The issue is patched in

Discourse version 2.8.4 on the `stable` branch and version `2.9.0.beta5` on the `beta` and `tests-passed` branches. As a workaround, disable invites or increase `min\_trust\_level\_to\_allow\_invite` to reduce the attack surface to more trusted users.

CVE-2022-31025 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [discourse](#) - **discourse** version < 2.8.4

Affected Vendor/Software: [discourse](#) - **discourse** version >= 2.9.0.beta1, <= 2.9.0.beta4

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	LOW	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

Description	Tags	Link
SECURITY: Remove auto approval when redeeming an invite (#16974) · discourse/discourse@7c4e2d3 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/7c4e2d3fa4b922354c177ffc880a2f2701a91f9
SECURITY: Remove auto approval when redeeming an invite by gschlager · Pull Request #16974 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/16974
Invite bypasses user approval · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-x7jh-mx5q-6f9q
FIX: Approves user when redeeming an invite for invites only sites by tgxworld · Pull Request #16984 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/16984
FIX: Approves user when redeeming an invite for invites only sites (#... · discourse/discourse@0fa0094 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/0fa0094531efc82d9371f90a02aa804b176d59cf

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	beta2	All	All
Application	Discourse	Discourse	2.9.0	beta3	All	All
Application	Discourse	Discourse	2.9.0	beta4	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:beta2:*.:*:*:*:*:						
cpe:2.3:a:discourse:discourse:2.9.0:beta3:*.:*:*:*:*:						

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-31025 : Discourse is an open source platform for community discussion. Prior to version 2.8.4 on the `stab... twitter.com/i/web/status/1...	2022-06-07 15:04:35
 /r/netcve	CVE-2022-31025	2022-06-07 16:38:24

[← 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](#)