

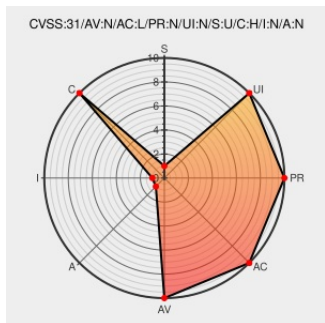


CVE-2021-41082

Published on: 09/20/2021 12:00:00 AM UTC

Last Modified on: 10/04/2021 06:07:00 PM UTC

CVE-2021-41082 - advisory for GHSA-vm3x-w6jm-j9vv

[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. In affected versions any private message that includes a group had its title and participating user exposed to users that do not have access to the private messages. However, access control for the private messages was not compromised as users were not able to view the posts in the leaked private message despite seeing it in their inbox. The problematic commit was reverted around 32 minutes after it was made. Users are encouraged to upgrade to the latest commit if they are running Discourse against the `tests-passed` branch.

CVE-2021-41082 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [discourse](#) - `discourse` version `>= tests-passed = ddb4583`, `< tests-passed = 27bad28`

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

CVE References

Description	Tags	Link
Group private messages title and participating users are leaked to users that do not have access. · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-vm3x-w6jm-j9vv
Partially revert "PERF: Improve query performance all inbox private m... · discourse/discourse@27bad28 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/27bad28c530c89acab35a56b945b6a3924280f4b
PERF: Improve query performance all inbox private messages. (#14304) · discourse/discourse@ddb4583 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/ddb458343dc39a7a8c99467dcd809b444514fe2c

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41082 : Discourse is a platform for community discussion. In affected versions any private message that in... twitter.com/i/web/status/1...	2021-09-20 20:25:20

← Previous ID

Next ID →

