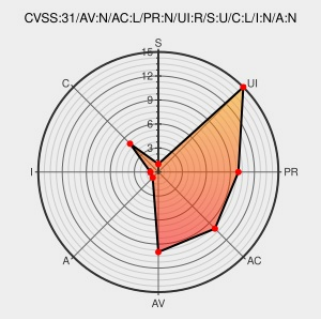
CVE-2021-37703

Published on: 08/13/2021 12:00:00 AM UTC

Last Modified on: 08/30/2021 11:08:00 AM UTC

CVE-2021-37703 - advisory for GHSA-gq2h-qhg2-phf9

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. In Discourse before versions 2.7.8 and 2.8.0.beta5, a user's read state for a topic such as the last read post number and the notification level is exposed.

CVE-2021-37703 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **< 2.7.8**

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
User's read state for a topic is leaked when unread state	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-gq2h-qhg2-phf9

message is published from the server to the clients. · Advisory · discourse/discourse · GitHub	text/html	phs
SECURITY: User's read state for topic is leaked to unauthorized clients. · discourse/discourse@aed65ec · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/aed65ec16d38886d7be7209d8c02df4ffd4937a4

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	2.8.0	beta1	All	All
Application	Discourse	Discourse	2.8.0	beta2	All	All
Application	Discourse	Discourse	2.8.0	beta3	All	All
Application	Discourse	Discourse	2.8.0	beta4	All	All

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

cpe:2.3:a:discourse:discourse:2.8.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.8.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.8.0:beta3:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.8.0:beta4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-37703 : Discourse is an open-source platform for community discussion. In Discourse before versions 2.7.8… twitter.com/i/web/status/1…	2021-08-13 15:22:34

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report