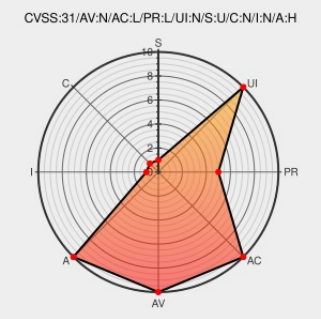
CVE-2022-39232

Published on: Not Yet Published

Last Modified on: 07/11/2023 09:02:00 PM UTC

CVE-2022-39232 - advisory for GHSA-cv64-v73f-7wq5

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. Starting with version 2.9.0.beta5 and prior to version 2.9.0.beta10, an incomplete quote can generate a JavaScript error which will crash the current page in the browser in some cases. Version 2.9.0.beta10 added a fix and tests to ensure incomplete quotes won't break the app. As a workaround, the quote can be fixed via the rails console.

CVE-2022-39232 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **>= 2.9.0.beta5, < 2.9.0.beta10**

CVSS3 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
SECURITY: Handle incomplete quote bbcode by CvX · Pull Request #18311 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/18311
Incomplete quote can cause a topic to crash in the browser · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-cv64-v73f-7wq5
SECURITY: Handle incomplete	github.com	MISC

quote bbcode (#18311) · discourse/discourse@eab33af · GitHub	text/html	github.com/discourse/discourse/commit/eab33af5bf19827527fe79134d865b5c727f6530

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	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: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-2022-39232 : Discourse is an open source discussion platform. Starting with version 2.9.0.beta5 and prior to ve… twitter.com/i/web/status/1…	2022-09-29 20:18:52
/r/netcve	CVE-2022-39232	2022-09-29 21:38:55

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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