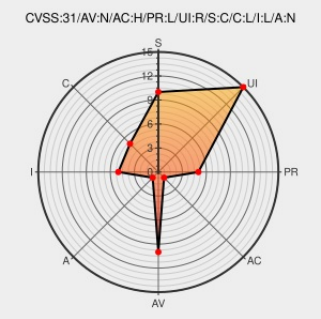
CVE-2021-39161

Published on: 08/26/2021 12:00:00 AM UTC

Last Modified on: 09/01/2021 04:58:00 PM UTC

CVE-2021-39161 - advisory for GHSA-xhmc-9jwm-wqph

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 affected versions category names can be used for Cross-site scripting(XSS) attacks. This is mitigated by Discourse's default Content Security Policy and this vulnerability only affects sites which have modified or disabled or changed Discourse's default Content Security Policy have allowed for moderators to modify categories. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.

CVE-2021-39161 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**

Affected Vendor/Software: **discourse** - **discourse** version **>= 2.8.0.beta1, < 2.8.0.beta4**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
XSS via category name · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-xhmc-9jwm-wqph

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	2.8.0	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-2021-39161 : Discourse is an open source platform for community discussion. In affected versions category names… twitter.com/i/web/status/1…	2021-08-26 20:09:15

← Previous ID Next ID→

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