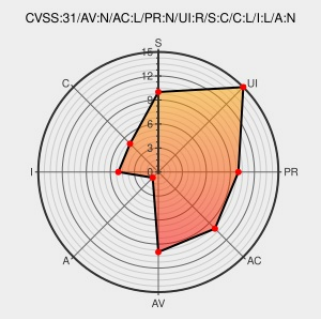
CVE-2023-29196

Published on: Not Yet Published

Last Modified on: 04/28/2023 03:50:00 AM UTC

CVE-2023-29196 - advisory for GHSA-986p-4x8q-8f48

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. This vulnerability is not exploitable on the default install of Discourse. A custom feature must be enabled for it to work at all, and the attacker's payload must pass the CSP to be executed. However, if an attacker succeeds in embedding Javascript that does pass the CSP, it could result in session hijacking for any users that view the attacker's post. The vulnerability is patched in the latest tests-passed, beta and stable branches. Users are advised to upgrade. Users unable to upgrade should enable and/or restore your site's CSP to the default one provided with Discourse. Remove any embed-able hosts configured.

CVE-2023-29196 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **= stable: < 3.0.3**

Affected Vendor/Software: **discourse** - **discourse** version **= beta: < 3.1.0.beta4**

CVSS3 Score: 6.1 - MEDIUM

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

CVE References

Description	Tags	Link
HTML injection via topic embedding · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-986p-4x8q-8f48

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	All	All	All	All
Application	Discourse	Discourse	3.1.0	beta1	All	All
Application	Discourse	Discourse	3.1.0	beta2	All	All
Application	Discourse	Discourse	3.1.0	beta3	All	All

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

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

cpe:2.3:a:discourse:discourse:3.1.0:beta1:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta2:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta3:*:*:beta:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-29196 : Discourse is an open source platform for community discussion. This vulnerability is not exploitab… twitter.com/i/web/status/1…	2023-04-18 22:03:44

← Previous ID

Next ID→