



Published on: Not Yet Published

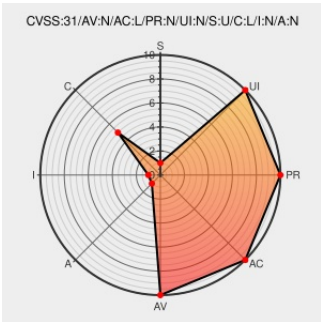
Last Modified on: 03/09/2023 09:11:00 PM UTC

CVE-2023-25819 - advisory for GHSA-xx2h-mwm7-hq6q

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. Tags that are normally private are showing in metadata. This affects any site running the `tests-passed` or `beta` branches $\geq 3.1.0.\text{beta}2$. The issue is patched in the latest `beta` and `tests-passed` version of Discourse.

CVE-2023-25819 has been assigned by  security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version = < 3.1.0.beta3

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
Tags with no visibility are leaking into og:article:tag · Advisory · discourse/discourse · GitHub	github.com text/html	 MISC github.com/discourse/discourse/security/advisories/GHSA-xx2h-mwm7-hq6q
SECURITY: Show only visible tags in metadata · discourse/discourse@a9f2c6d · GitHub	github.com text/html	 MISC github.com/discourse/discourse/commit/a9f2c6db64e7d78b8e0f55e7bd77c5fe3459b831

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

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	3.1.0	beta1	All	All
Application	Discourse	Discourse	3.1.0	beta2	All	All
cpe:2.3:a:discourse:discourse:****.***.*:						
cpe:2.3:a:discourse:discourse:3.1.0:beta1:*.*:beta:***.*:						
cpe:2.3:a:discourse:discourse:3.1.0:beta2:*.*:beta:***.*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-25819 : Discourse is an open source platform for community discussion. Tags that are normally private are... twitter.com/i/web/status/1...	2023-03-04 01:07:08
 /r/netcve	CVE-2023-25819	2023-03-04 02:38:16
 /r/AJsBotPlayground	[MEDIUM] CVE Report on March 10, 2023 12:14 [1/3]	2023-03-10 12:14:44
 /r/AJsBotPlayground	[MEDIUM] CVE Report on March 10, 2023 11:59 [1/3]	2023-03-10 11:59:21

[← Previous ID](#)

[Next ID →](#)

© CVEreport 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVEreport and Source URL Uptime Status [status.cve.report](#)