

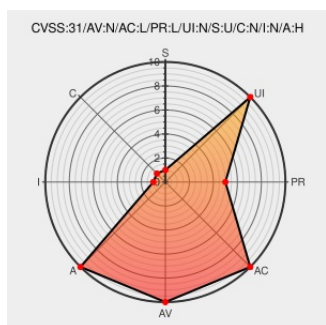


CVE-2023-22739

Published on: Not Yet Published

Last Modified on: 02/06/2023 05:03:00 PM UTC

CVE-2023-22739 - advisory for GHSA-rqgr-g6v7-jcfc

[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. Versions prior to 3.0.1 (stable), 3.1.0.beta2 (beta), and 3.1.0.beta2 (tests-passed) are subject to Allocation of Resources Without Limits or Throttling. As there is no limit on data contained in a draft, a malicious user can create an arbitrarily large draft, forcing the instance to a crawl.

This issue is patched in versions 3.0.1 (stable), 3.1.0.beta2 (beta), and 3.1.0.beta2 (tests-passed). There are no workarounds.

CVE-2023-22739 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [discourse](#) - **discourse** version = **stable** < 3.0.1

Affected Vendor/Software: [discourse](#) - **discourse** version = **beta** < 3.1.0.beta2

Affected Vendor/Software: [discourse](#) - **discourse** version = **tests-passed** <3.1.0.beta2

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
DOS through topic drafts · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-rqgr-g6v7-jcfc

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-22739 : Discourse is an open source platform for community discussion. Versions prior to 3.0.1 stable , 3... twitter.com/i/web/status/1...	2023-01-26 22:02:27

[← Previous ID](#)

Next ID→

© CVE.report 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](#).

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