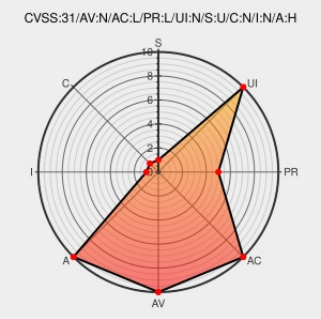
CVE-2023-22740

Published on: Not Yet Published

Last Modified on: 02/06/2023 07:30:00 PM UTC

CVE-2023-22740 - advisory for GHSA-pwj4-rf62-p224

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 3.1.0.beta1 (beta) (tests-passed) are vulnerable to Allocation of Resources Without Limits. Users can create chat drafts of an unlimited length, which can cause a denial of service by generating an excessive load on the server. Additionally, an unlimited number of drafts were loaded when loading the user. This issue has been patched in version 2.1.0.beta1 (beta) and (tests-passed). Users should upgrade to the latest version where a limit has been introduced. There are no workarounds available.

CVE-2023-22740 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **= beta < 3.1.0.beta1; tests-passed < 3.1.0.beta1**

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
Chat drafts should have a maximum character limit and the number of loaded drafts should be limited · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-pwj4-rf62-p224
SECURITY: Limit chat drafts length	github.com	MISC

and preloaded count (#19987) · discourse/discourse@5eaf080 · GitHub	text/html	github.com/discourse/discourse/commit/5eaf0802398ff06604f03b27a28dd274f2ffa576

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Discourse is an open source platform for community discussion. Versions prior to 3.1.0.beta1 (beta) (tests-passed) ar…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Discourse	Discourse	All	All	All	All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-22740 : Discourse is an open source platform for community discussion. Versions prior to 3.1.0.beta1 beta… twitter.com/i/web/status/1…	2023-01-27 01:07:18

← Previous ID

Next ID→