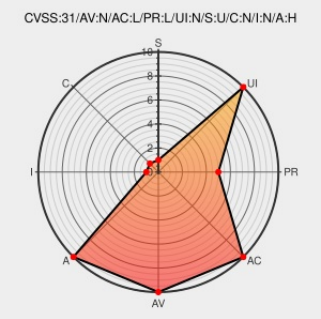
CVE-2023-38706

Published on: Not Yet Published

Last Modified on: 09/20/2023 07:59:00 PM UTC

CVE-2023-38706 - advisory for GHSA-7wpp-4pqg-gvp8

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Discourse from Discourse contain the following vulnerability:

Discourse is an open-source discussion platform. Prior to version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches, a malicious user can create an unlimited number of drafts with very long draft keys which may end up exhausting the resources on the server. The issue is patched in version 3.1.1 of the `stable` branch and version 3.2.0.beta1 of the `beta` and `tests-passed` branches. There are no known workarounds.

CVE-2023-38706 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version = **stable < 3.1.1**

Affected Vendor/Software: **discourse** - **discourse** version = **beta < 3.2.0.beta1**

Affected Vendor/Software: **discourse** - **discourse** version = **tests-passed < 3.2.0.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
DoS via drafts · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-7wpp-4pqg-gvp8

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
Application	Discourse	Discourse	3.1.0	beta2	All	All
Application	Discourse	Discourse	3.1.0	beta3	All	All
Application	Discourse	Discourse	3.1.0	beta5	All	All
Application	Discourse	Discourse	3.1.0	beta6	All	All
Application	Discourse	Discourse	3.1.0	beta7	All	All
Application	Discourse	Discourse	3.1.0	beta8	All	All
Application	Discourse	Discourse	All	All	All	All

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

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:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta5:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta6:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta7:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta8:*:*:beta:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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