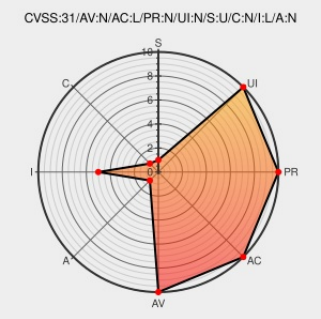
CVE-2023-32061

Published on: Not Yet Published

Last Modified on: 06/23/2023 02:07:00 AM UTC

CVE-2023-32061 - advisory for GHSA-prx4-49m8-874g

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 3.0.4 of the `stable` branch and version 3.1.0.beta5 of the `beta` and `tests-passed` branches, the lack of restrictions on the iFrame tag makes it easy for an attacker to exploit the vulnerability and hide subsequent comments from other users. This issue is patched in version 3.0.4 of the `stable` branch and version 3.1.0.beta5 of the `beta` and `tests-passed` branches. There are no known workarounds.

CVE-2023-32061 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **= < 3.0.4**

Affected Vendor/Software: **discourse** - **discourse** version **= >= 3.1.0.beta1, < 3.1.0.beta5**

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	NONE	LOW	NONE

CVE References

Description	Tags	Link
Topic Creation Page Allows iFrame Tag without Restrictions · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-prx4-49m8-874g

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	beta4	All	All

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:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta4:*:*:beta:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→