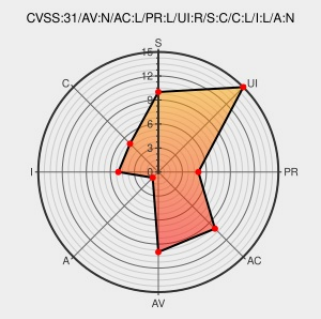
CVE-2023-25172

Published on: Not Yet Published

Last Modified on: 03/23/2023 08:40:00 PM UTC

CVE-2023-25172 - advisory for GHSA-7pm2-prxw-wrvp

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 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included in a user's full name field to to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse.

CVE-2023-25172 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: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
XSS user name displayed on post	github.com	MISC github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp

· Advisory · discourse/discourse · GitHub	text/html	
SECURITY: Prevent XSS in local oneboxes (#20009) · discourse/discourse@1a5a6f6 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915
SECURITY: Prevent XSS in local oneboxes by nbianca · Pull Request #20009 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/20009
SECURITY: Prevent XSS in local oneboxes (#20008) · discourse/discourse@c186a46 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/c186a46910431020e8efc425dec2133e7a99fa9a
SECURITY: Prevent XSS in local oneboxes by nbianca · Pull Request #20008 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/20008

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	All	All	All	All
Application	Discourse	Discourse	3.1.0	beta1	All	All

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

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

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-2023-25172 : Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and… twitter.com/i/web/status/1…	2023-03-17 17:01:50
/r/netcve	CVE-2023-25172	2023-03-17 17:38:05

← Previous ID

Next ID→