



# CVE-2023-25172

Published on: Not Yet Published

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

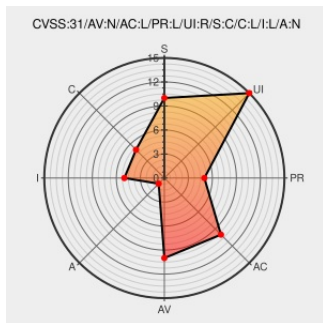
## CVE-2023-25172 - advisory for GHSA-7pm2-prxw-wrvp

[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 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](mailto: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
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

### CVE References

Description	Tags	Link
XSS user name displayed on post		<a href="https://github.com">github.com</a> <a href="https://github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp">MISC github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp</a>

· 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/1a5a6f6cb821ed29a737311d6fdc2eba5adc915

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

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](mailto: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	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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2023-03-17 17:01:50
/r/netcve	<a href="#">CVE-2023-25172</a>	2023-03-17 17:38:05

← 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](https://status.cve.report)**