

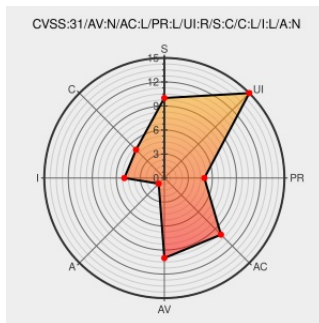


CVE-2022-39270

Published on: Not Yet Published

Last Modified on: 11/10/2022 04:15:00 AM UTC

CVE-2022-39270 - advisory for GHSA-m44p-w923-w32h

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Discotoc](#) from [Discourse](#) contain the following vulnerability:

DiscoTOC is a Discourse theme component that generates a table of contents for topics. Users that can create topics in TOC-enabled categories (and have sufficient trust level - configured in component's settings) are able to inject arbitrary HTML on that topic's page. The issue has been fixed on the `main` branch. Admins can update the

theme component through the admin UI (Customize -> Themes -> Components -> DiscoTOC -> Check for Updates). Alternatively, admins can temporarily disable the DiscoTOC theme component.

CVE-2022-39270 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: discourse - DiscoTOC version < 2.1.0

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
SECURITY: Render TOC items as plain text (#44) · discourse/DiscoTOC@f80c215 · GitHub	github.com text/html	MISC github.com/discourse/DiscoTOC/commit/f80c215a283cd045d2a371403e6eba88b2911192
cve-website	www.cve.org text/html	MISC www.cve.org/CVERecord?id=CVE-2022-39270

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	Discotoc	All	All	All	All
cpe:2.3:a:discourse:discotoc:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID →		