

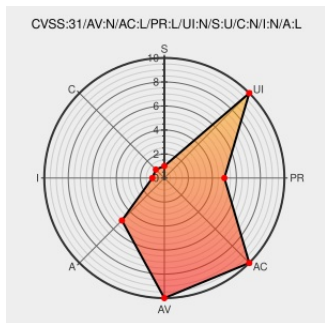


CVE-2021-43827

Published on: Not Yet Published

Last Modified on: 12/29/2021 08:31:00 PM UTC

CVE-2021-43827 - advisory for GHSA-58vr-c56v-qr57

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

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

discourse-footnote is a library providing footnotes for posts in Discourse. ### Impact When posting an inline footnote wrapped in `` tags (e.g. `^[footnote]</a>`), the resulting rendered HTML would include a nested ``, which is stripped by Nokogiri because it is not valid. This then caused a javascript error on topic pages because

we were looking for an `` element inside the footnote reference span and getting its ID, and because it did not exist we got a null reference error in javascript. Users are advised to update to version 0.2. As a workaround editing offending posts from the rails console or the database console for self-hosters, or disabling the plugin in the admin panel can mitigate this issue.

CVE-2021-43827 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: discourse - discourse-footnote version < 0.2

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	LOW

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

PARTIAL

CVE References

Description	Tags	Link
SECURITY: Fix malicious footnote causing clientside errors (#27) · discourse/discourse-footnote@796617e · GitHub	github.com text/html	MISC github.com/discourse/discourse-footnote/commit/796617e0131277011207541313522cd1946661ab
Malicious footnote markup may cause client side errors. · Advisory · discourse/discourse-footnote · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse-footnote/security/advisories/GHSA-58vr-c56v-qr57

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 Footnote	All	All	All	All
cpe:2.3:a:discourse:discourse_footnote:***:***:discourse:***						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2021-43827	2021-12-14 23:38:09

[← 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](#)