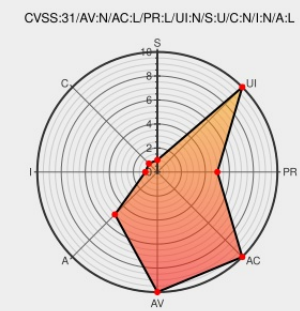
CVE-2021-43827

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 `<a>` tags (e.g. `<a>^[footnote]</a>`, the resulting rendered HTML would include a nested `<a>`, 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 `<a>` 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/796617e013127701120754131352 2cd1946661ab
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

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→