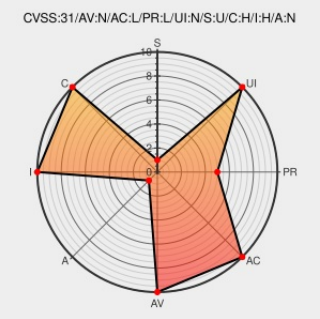
CVE-2021-32764

Published on: 07/15/2021 12:00:00 AM UTC

Last Modified on: 09/13/2021 02:44:00 PM UTC

CVE-2021-32764 - advisory for GHSA-9x4c-29xg-56hw

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. In Discourse versions 2.7.5 and prior, parsing and rendering of YouTube Oneboxes can be susceptible to XSS attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. The issue is patched in `stable` version 2.7.6, `beta` version 2.8.0.beta3, and `tests-passed` version 2.8.0.beta3. As a workaround, ensure that the Content Security Policy is enabled, and has not been modified in a way which would make it more vulnerable to XSS attacks.

CVE-2021-32764 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **discourse** - **discourse** version **<= 2.7.5**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
YouTube Onebox susceptible to XSS · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-9x4c-29xg-56hw

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	2.8.0	beta1	All	All
Application	Discourse	Discourse	All	All	All	All

cpe:2.3:a:discourse:discourse:2.8.0:beta1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32764 : Discourse is an open-source discussion platform. In Discourse versions 2.7.5 and prior, parsing an… twitter.com/i/web/status/1…	2021-07-15 20:45:43
/r/netcve	CVE-2021-32764	2021-07-15 21:41:19

← Previous ID

Next ID→