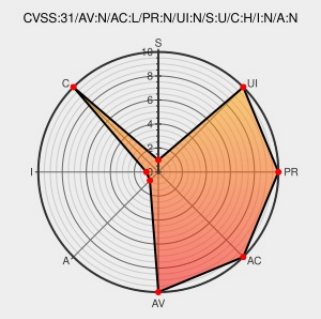
CVE-2023-28111

Published on: Not Yet Published

Last Modified on: 03/23/2023 08:57:00 PM UTC

CVE-2023-28111 - advisory for GHSA-26h3-8ww8-v5fc

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 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's server-side request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of Discourse. version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.

CVE-2023-28111 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **discourse** - **discourse** version **= beta < 3.1.0.beta3**

Affected Vendor/Software: **discourse** - **discourse** version **= tests-passed < 3.1.0.beta3**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
SECURITY: Multiple commits for version bump beta3 by oblakeerickson · Pull Request #20710 · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/pull/20710
SECURITY: SSRF protection	github.com	MISC

bypass with IPv4-mapped IPv6 addresses · discourse/discourse@fd16ead · GitHub	text/html	github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a
SSRF protection bypass possible with IPv4-mapped IPv6 addresses · Advisory · discourse/discourse · GitHub	github.com text/html	MISC github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc

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	3.1.0	beta1	All	All
Application	Discourse	Discourse	3.1.0	beta2	All	All

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

cpe:2.3:a:discourse:discourse:3.1.0:beta1:*:*:beta:*:*:*:

cpe:2.3:a:discourse:discourse:3.1.0:beta2:*:*:beta:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28111 : Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `t… twitter.com/i/web/status/1…	2023-03-17 17:02:17
/r/netcve	CVE-2023-28111	2023-03-17 17:38:07

← Previous ID

Next ID→