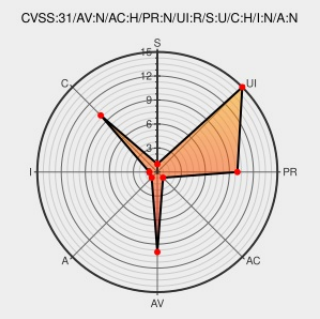
CVE-2021-37693

Published on: 08/13/2021 12:00:00 AM UTC

Last Modified on: 08/30/2021 06:01:00 PM UTC

CVE-2021-37693 - advisory for GHSA-9377-96f4-cww4

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Discourse from Discourse contain the following vulnerability:

Discourse is an open-source platform for community discussion. In Discourse before versions 2.7.8 and 2.8.0.beta4, when adding additional email addresses to an existing account on a Discourse site an email token is generated as part of the email verification process. Deleting the additional email address does not invalidate an unused token which can then be used in other contexts, including reseting a password.

CVE-2021-37693 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **discourse** - **discourse** version **< 2.7.8**

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	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

Re-use of email tokens · Advisory · discourse/discourse · GitHub	github.com text/html	CONFIRM github.com/discourse/discourse/security/advisories/GHSA-9377-96f4-cww4
SECURITY: Destroy `EmailToken` when `EmailChangeRequest` is destroyed… · discourse/discourse@fb14e50 · GitHub	github.com text/html	MISC github.com/discourse/discourse/commit/fb14e50741a4880cda22244eded8858e2f5336ef

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	2.8.0	beta1	All	All
Application	Discourse	Discourse	2.8.0	beta2	All	All
Application	Discourse	Discourse	2.8.0	beta3	All	All

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

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

cpe:2.3:a:discourse:discourse:2.8.0:beta2:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.8.0:beta3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-37693 : Discourse is an open-source platform for community discussion. In Discourse before versions 2.7.8… twitter.com/i/web/status/1…	2021-08-13 15:16:14

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report