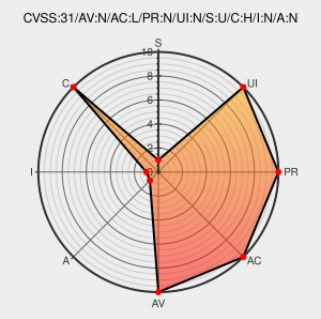
CVE-2021-3138

Published on: 01/13/2021 12:00:00 AM UTC

Last Modified on: 01/04/2022 04:36:00 PM UTC

CVE-2021-3138

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



Certain versions of Discourse from Discourse contain the following vulnerability:

In Discourse 2.7.0 through beta1, a rate-limit bypass leads to a bypass of the 2FA requirement for certain forms.

CVE-2021-3138 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Discourse 2.7.0 2FA Bypass ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162256/Discourse-2.7.0-2FA-Bypass.html
GitHub - Mesh3l911/Discourse: Disource POC	Third Party Advisory github.com	MISC github.com/Mesh3l911/Disource

	text/html	
Releases · discourse/discourse · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/discourse/discourse/releases

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Discource POC

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Discourse	Discourse	2.7.0	beta1	All	All
Application	Discourse	Discourse	2.7.0	beta1	All	All
Application	Discourse	Discourse	All	All	All	All

cpe:2.3:a:discourse:discourse:2.7.0:beta1:*:*:*:*:*:*:

cpe:2.3:a:discourse:discourse:2.7.0:beta1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Mesh3l_911	صبّحكم الله بالخير ، Write-up: Recon > Code Review > 0day > CVE-2021–3138 > Apple HOF دعواتكم♥?? medium.com/@Mesh3l_911/re…	2021-04-03 01:21:21
@softek_jp	Juniper Networks Junos OS にファイアウォールフィルタを意図しないインターフェイスへ適用する問題 (CVE-2021-3138 [40260] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-15 06:00:16

← Previous ID

Next ID→

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