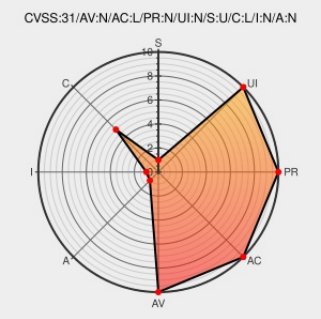
CVE-2020-8278

Published on: 11/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8278

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



Certain versions of Social from Nextcloud contain the following vulnerability:

Improper access control in Nextcloud Social app version 0.3.1 allowed to read posts of any user.

CVE-2020-8278 has been assigned by support@hackerone.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	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
HackerOne	Exploit Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/921717

advisory – Nextcloud	Broken Link Product nextcloud.com text/html	CONFIRM nextcloud.com/security/advisory/?id=NC-SA-2020-042

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Social	0.3.1	All	All	All
Application	Nextcloud	Social	0.3.1	All	All	All

cpe:2.3:a:nextcloud:social:0.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:nextcloud:social:0.3.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→