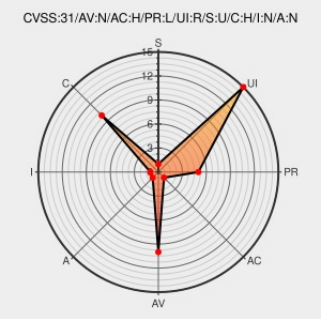
CVE-2021-39223

Published on: 10/25/2021 12:00:00 AM UTC

Last Modified on: 10/29/2021 02:43:00 PM UTC

CVE-2021-39223 - advisory for GHSA-rjcc-4cgj-6v93

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



Certain versions of Richdocuments from Nextcloud contain the following vulnerability:

Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Richdocuments application prior to versions 3.8.6 and 4.2.3 returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. (e.g. an attacker could see that the file `shared.txt` is located within `/files/$username/Myfolder/Mysubfolder/shared.txt`). It is recommended that the Richdocuments application is upgraded to 3.8.6 or 4.2.3. As a workaround, disable the Richdocuments application in the app settings.

CVE-2021-39223 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **< 3.8.6,**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **>= 4.0.0, < 4.2.3**

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	hackerone.com text/html	MISC hackerone.com/reports/1253460
Unify error messages accross controllers by juliushaertl · Pull Request #1760 · nextcloud/richdocuments · GitHub	github.com text/html	MISC github.com/nextcloud/richdocuments/pull/1760
File path disclosure of shared files in Richdocuments application · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	CONFIRM github.com/nextcloud/security-advisories/security/advisories/GHSA-rjcc-4cgj-6v93

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Richdocuments	All	All	All	All

cpe:2.3:a:nextcloud:richdocuments:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39223 : Nextcloud is an open-source, self-hosted productivity platform. The Nextcloud Richdocuments applic… twitter.com/i/web/status/1…	2021-10-25 21:39:11

← Previous ID

Next ID→