

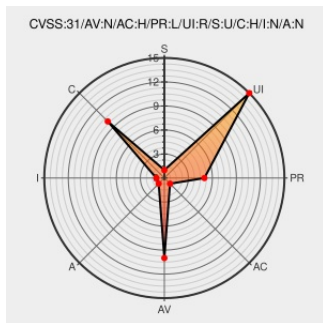


CVE-2021-39223

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/Myfolder/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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)