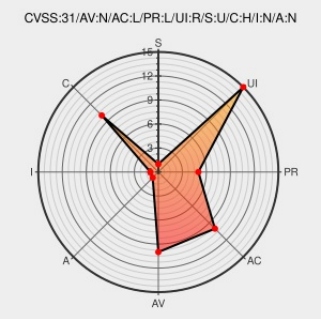
CVE-2023-25150

Published on: Not Yet Published

Last Modified on: 02/16/2023 10:20:00 PM UTC

CVE-2023-25150 - advisory for GHSA-64xc-r58v-53gj

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



Certain versions of Richdocuments from Nextcloud contain the following vulnerability:

Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabora integration can be tricked to provide access to any file without proper permission validation. As a result any user with access to Collabora can obtain the content of other users files. It is recommended that the Nextcloud Office App (Collabora Integration) is updated to 7.0.2 (Nextcloud 25), 6.3.2 (Nextcloud 24), 5.0.10 (Nextcloud 23), 4.2.9 (Nextcloud 21-22), or 3.8.7 (Nextcloud 15-20). There are no known workarounds for this issue.

CVE-2023-25150 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= < 3.8.7**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 4.0.0, < 4.2.9**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 5.0.0, < 5.0.10**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 6.0.0, < 6.3.2**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 7.0.0, < 7.0.2**

CVSS3 Score: 5.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Move WOPI checks to the middleware by juliushaertl · Pull Request #2669 · nextcloud/richdocuments · GitHub	github.com text/html	MISC github.com/nextcloud/richdocuments/pull/2669
Document content of files can be obtained through Collabora for files of other users · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-64xc-r58v-53gj
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1788222

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

Exploit/POC from Github

Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected versions the Collabor…

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-2023-25150 : Nextcloud office/richdocuments is an office suit for the nextcloud server platform. In affected ve… twitter.com/i/web/status/1…	2023-02-08 20:03:53
/r/netcve	CVE-2023-25150	2023-02-08 21:38:47

← 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 registred 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