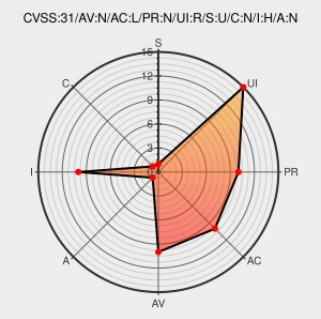
CVE-2022-31024

Published on: Not Yet Published

Last Modified on: 06/13/2022 04:20:00 PM UTC

CVE-2022-31024 - advisory for GHSA-94hr-7g4v-f53r

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



Certain versions of Richdocuments from Nextcloud contain the following vulnerability:

richdocuments is the repository for NextCloud Collabra, the app for Nextcloud Office collaboration. Prior to versions 6.0.0, 5.0.4, and 4.2.6, a user could be tricked into working against a remote Office by sending them a federated share. richdocuments versions 6.0.0, 5.0.4 and 4.2.6 contain a fix for this issue. There are currently no known workarounds available.

CVE-2022-31024 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **< 4.2.6**

Affected Vendor/Software: **nextcloud** - **security-advisories** version **>= 5.0.0, < 5.0.4**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1210424
Add app config to enable trusted domain list usage by juliushaertl · Pull Request #2161 · nextcloud/richdocuments · GitHub	github.com text/html	MISC github.com/nextcloud/richdocuments/pull/2161
Federated editing allows iframing remote servers by default · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	CONFIRM github.com/nextcloud/security-advisories/security/advisories/GHSA-94hr-7g4v-f53r

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
Application	Nextcloud	Richdocuments	6.0.0	beta1	All	All

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

cpe:2.3:a:nextcloud:richdocuments:6.0.0:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-31024	2022-06-02 19:38:38

← Previous ID

Next ID→