

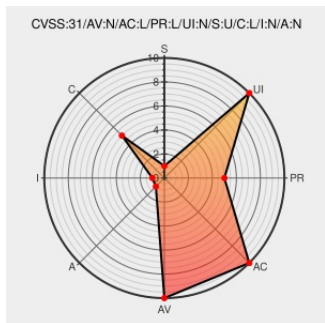


CVE-2023-28834

Published on: Not Yet Published

Last Modified on: 04/10/2023 01:56:00 PM UTC

CVE-2023-28834 - advisory for GHSA-5w64-6c42-rgcv

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Nextcloud Server](#) from [Nextcloud](#) contain the following vulnerability:

Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and 25.0.0 until 25.0.4, as well as Nextcloud Enterprise Server 23.0.0 until 23.0.11, 24.0.0 until 24.0.6, and 25.0.0 until 25.0.4, have an information disclosure vulnerability. A user was able to get the full data directory path of the Nextcloud server from an

API endpoint. By itself this information is not problematic as it can also be guessed for most common setups, but it could speed up other unknown attacks in the future if the information is known. Nextcloud Server 24.0.6 and 25.0.4 and Nextcloud Enterprise Server 23.0.11, 24.0.6, and 25.0.4 contain patches for this issue. There are no known workarounds.

CVE-2023-28834 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [nextcloud](#) - [security-advisories](#) version = `>= 23.0.0, < 23.0.14`

Affected Vendor/Software: [nextcloud](#) - [security-advisories](#) version = `>= 24.0.0, < 24.0.10`

Affected Vendor/Software: [nextcloud](#) - [security-advisories](#) version = `>= 25.0.0, < 25.0.4`

CVSS3 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
[Bug]: the complete server installation path is visible in cloud/user	github.com	MISC

endpoint · Issue #33883 · nextcloud/server · GitHub	text/html	github.com/nextcloud/server/issues/33883
HackerOne	hackerone.com text/html	h MISC hackerone.com/reports/1690510
Only expose storage location to admins by PVince81 · Pull Request #36094 · nextcloud/server · GitHub	github.com text/html	MISC github.com/nextcloud/server/pull/36094
Full path of data directory exposed to users · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-5w64-6c42-rgcv

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	Nextcloud Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:						
cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:enterprise:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-28834 : Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and... twitter.com/i/web/status/1...	2023-04-03 17:05:10
 /r/netcve	CVE-2023-28834	2023-04-03 18:38:26
 /r/Team_IT_Security	CVE-2023-28834	2023-04-03 18:24:03

[← Previous ID](#)

[Next ID →](#)

