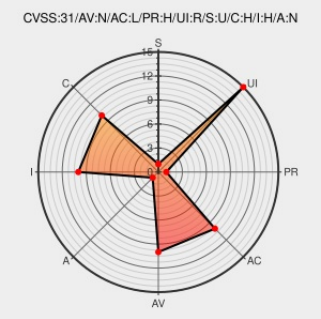
CVE-2023-28998

Published on: Not Yet Published

Last Modified on: 04/10/2023 06:14:00 PM UTC

CVE-2023-28998 - advisory for GHSA-jh3g-wpwv-cqgr

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



Certain versions of Desktop from Nextcloud contain the following vulnerability:

The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.6.5, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure, and add new files. Users should upgrade the Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are available.

CVE-2023-28998 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **= >= 3.0.0, < 3.6.5**

CVSS3 Score: 6.1 - MEDIUM

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

CVE References

Description	Tags	Link
Desktop clients misbehaves with end-to-end encryption when the server returns an empty list of metadata keys · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-jh3g-wpwv-cqgr
Bugfix/e2ee vulnerability empty metadatakeys by allexzander · Pull Request #5323 · nextcloud/desktop · GitHub	github.com text/html	MISC github.com/nextcloud/desktop/pull/5323
	ethz.ch application/pdf	MISC ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/appliedcrypto/education/theses/report_DanieleCoppola.pdf

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.

Related QID Numbers

183259 Debian Security Update for nextcloud-desktop (CVE-2023-28998)

503201 Alpine Linux Security Update for nextcloud-client

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:nextcloud:desktop:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28998 : The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with v… twitter.com/i/web/status/1…	2023-04-04 13:07:29
/r/netcve	CVE-2023-28998	2023-04-04 14:38:53

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report