

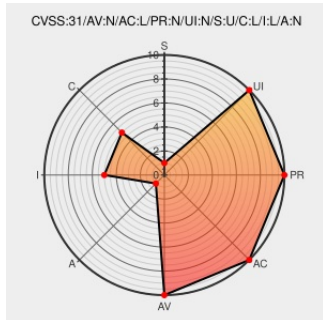


CVE-2023-29000

Published on: Not Yet Published

Last Modified on: 04/11/2023 02:52:00 PM UTC

CVE-2023-29000 - advisory for GHSA-h82x-98q3-7534

[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 3.7.0, by trusting that the server will return a certificate that belongs to the keypair of the user, a malicious server could get the desktop client to encrypt files with a key known to the attacker. This issue is fixed in Nextcloud Desktop 3.7.0. No known workarounds are available.

CVE-2023-29000 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, < 3.7.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1679267
validate certificate for E2EE against private key by mgallien · Pull Request #4949 · nextcloud/desktop · GitHub	github.com text/html	MISC github.com/nextcloud/desktop/pull/4949
Desktop client does not verify received signed certificate in end-to-end encryption · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-h82x-98q3-7534

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

182630 Debian Security Update for nextcloud-desktop (CVE-2023-29000)

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-2023-29000 : 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 13:08:25
 /r/netcve	CVE-2023-29000	2023-04-04 14:38:54

[← 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