



CVE-2023-28997

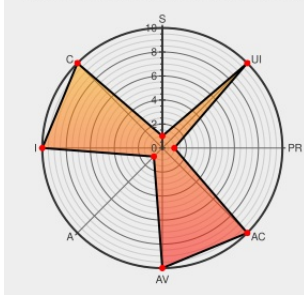
Published on: Not Yet Published

Last Modified on: 04/10/2023 05:48:00 PM UTC

CVE-2023-28997 - advisory for GHSA-4p33-rw27-j5fc

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

CVSS:31/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N



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 recover and modify the contents of end-to-end encrypted files. Users should upgrade the Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are

available.

CVE-2023-28997 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: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Initialization vector reuse in end-to-end encryption allows a malicious server admin to break manipulate and access files · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	MISC github.com/nextcloud/security-advisories/security/advisories/GHSA-4p33-rw27-j5fc
Always generate random initialization vector when uploading encrypted file by allexzander · Pull Request #5324 · nextcloud/desktop · GitHub	github.com text/html	MISC github.com/nextcloud/desktop/pull/5324
	ethz.ch	MISC ethz.ch/content/dam/ethz/special-interest/infk/inst-

comment@cve.report.

Related QID Numbers

182122 Debian Security Update for nextcloud-desktop (CVE-2023-28997)

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
<code>cpe:2.3:a:nextcloud:desktop:*.*.*.*.*.*.*.*.</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-28997 : 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 13:07:01
 /r/netcve	CVE-2023-28997	2023-04-04 14:38:52
 /r/Team_IT_Security	CVE-2023-28997	2023-04-04 23:07:27

[← Previous ID](#)

Next ID→