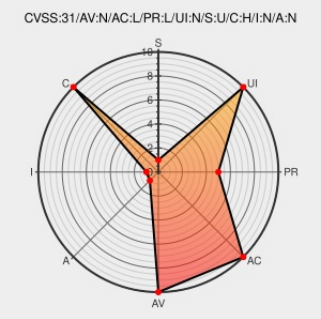
CVE-2021-32728

Published on: 08/18/2021 12:00:00 AM UTC

Last Modified on: 10/04/2022 02:14:00 PM UTC

CVE-2021-32728 - advisory for GHSA-f5fr-5gcv-6cc5

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with a computer. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.3.0, the Nextcloud Desktop client fails to check if a private key belongs to previously downloaded public certificate. If the Nextcloud instance serves a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. This issue is fixed in Nextcloud Desktop Client version 3.3.0. There are no known workarounds aside from upgrading.

CVE-2021-32728 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **< 3.3.0**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4974-1 nextcloud-desktop	www.debian.org Depreciated Link text/html	DEBIAN DSA-4974
check e2ee public key against private one by mgallien · Pull Request #3338 · nextcloud/desktop · GitHub	github.com text/html	MISC github.com/nextcloud/desktop/pull/3338
End-to-end encryption device setup did not verify public key · Advisory · nextcloud/security-advisories · GitHub	github.com text/html	CONFIRM github.com/nextcloud/security-advisories/security/advisories/GHSA-f5fr-5gcv-6cc5
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1189162

Related QID Numbers

178799 Debian Security Update for nextcloud-desktop (DSA 4974-1)

183383 Debian Security Update for nextcloud-desktop (CVE-2021-32728)

Exploit/POC from Github

The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with a computer. Clients using the …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Nextcloud	Desktop	All	All	All	All
Application	Nextcloud	Nextcloud	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32728 : The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with a computer.… twitter.com/i/web/status/1…	2021-08-18 16:02:11

← Previous ID

Next ID→