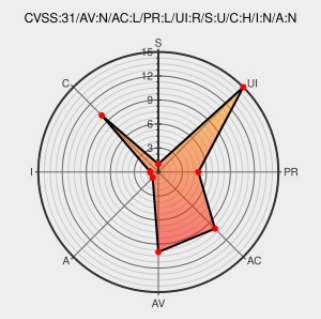
CVE-2021-32727

Published on: 07/12/2021 12:00:00 AM UTC

Last Modified on: 07/14/2021 01:23:00 PM UTC

CVE-2021-32727 - advisory for GHSA-5v33-r9cm-7736

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



Certain versions of Nextcloud from Nextcloud contain the following vulnerability:

Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account.

CVE-2021-32727 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **nextcloud** - **security-advisories** version **< 3.16.1**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
end_to_end_encryption_rfc/RFC.md at 7f002996397faefb664019a97ebb0a1e210f64f0 · nextcloud/end_to_end_encryption_rfc · GitHub	github.com text/html	MISC github.com/nextcloud/end_to_end_encryption_rfc/blob/7f002996397faefb6 devices
check e2e keys by tobiasKaminsky · Pull Request #8438 · nextcloud/android · GitHub	github.com text/html	MISC github.com/nextcloud/android/pull/8438
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1189162
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

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32727 : Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-e… twitter.com/i/web/status/1…	2021-07-12 20:45:57
/r/netcve	CVE-2021-32727	2021-07-12 21:41:31

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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