8 com.nextcloud.client bypass the protection lock in andoid app v 3.18.1 latest version.

Share:

SUMMARY BY NEXTCLOUD

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-32j4-9xf3-h2mg

TIMELINE

dashingjaved submitted a report to Nextcloud. Jan 15th (11 months ago)

Summary:

nextcloud allowed multiple account within the android client app on a single lock

Steps To Reproduce:

1.open nextcloud app
2.add security password to protect the app
3.close the app
again open the app and now show the password to open the app

1. so now the password protection bypass lets start 2.hold the nextcloud app and see the app info open it 3.Here the three option 1.open.2.uninstall and 3.force stop now click open button and now see the app lock protection in the app and now open app and back open and back between 3 to 4 time same procedure and now you will see the app lock protection bypass in nextcloud android app

Supporting Material/References:

[list any additional material (e.g. screenshots, logs, etc.)]

- [attachment / reference]

Impact

regards.Javed Ahmad

1 attachment:
F1580106: WhatsApp_Video_2022-01-15_at_5.44.07_PM.mp4

dashingjaved posted a comment. Jan 17th (10 months ago)
Any update?

OT: posted a comment. Jan 18th (10 months ago)
Thanks a lot for reporting this potential issue back to us!

Our security team will take a look at this issue as soon as possible. For obvious reasons we'd like to ask you to not disclose this issue to any other party.

nickvergessen Nextcloud staff changed the status to ○ **Triaged**. Jan 18th (10 months ago)
Forwarded to the client team, thanks for the video!

nickvergessen Nextcloud staff posted a comment. Jan 19th (10 months ago)
We fail to reproduce this.
Can you tell us the Android version and the used device?

dashingjaved posted a comment. Jan 19th (10 months ago)
Yeah, in the initial poc i used OnePlus 9 pro which is based on android 11,

I have also attached a video poc which uses Oppo Find X2 based on android 11.

To reproduce the issue you have to quickly do the steps as I shown in the video poc.

Best regards,

1 attachment:
F1584452: VID-20220119-WA0003.mp4

dashingjaved posted a comment. Jan 22nd (10 months ago)
Any updates???

dashingjaved posted a comment. Jan 29th (10 months ago)

After long time in no response for security team.
Any Update???

nickvergessen Nextcloud staff posted a comment. Jan 31st (10 months ago)

The team managed to reproduce something on a single device and will follow up once we have more information.

dashingjaved posted a comment. Jan 31st (10 months ago)

Hey security team I also checked in another device just like a mi A1 device based on android 9,
Vivo v15 based on android 11 and tecno spark 6 go based on android 10.

dashingjaved posted a comment. Feb 9th (10 months ago)

any update?

nickvergessen Nextcloud staff posted a comment. Feb 10th (10 months ago)

A patch is being worked on. If you want you can try the build from https://github.com/nextcloud/android/pull/9816

dashingjaved posted a comment. Feb 11th (10 months ago)

Hey security team i tested this issue and yes now the problem is fixed.
Thanks for fixing.

dashingjaved posted a comment. Feb 19th (9 months ago)

Any Updates?

nickvergessen Nextcloud staff closed the report and changed the status to ○ **Resolved**. Feb 21st (9 months ago)

Thanks a lot for your report again. This has been resolved in our upcoming maintenance releases and we're working on the advisories at the moment.

If you have a GitHub account please let us know the username, and we will associate it with the advisory.

dashingjaved posted a comment. Mar 15th (9 months ago)

https://github.com/kaifhaxor hear is my GitHub account sorry for delay.

dashingjaved posted a comment. Mar 17th (8 months ago)

Any bounty reward???

dashingjaved posted a comment. Mar 20th (8 months ago)

Hey security team after long time no advisory for me and no response in my comments?

nickvergessen Nextcloud staff posted a comment. Mar 21st (8 months ago)

Hi there, I'm currently on-boarding new colleagues to the process. it will just take a little more time ~1-2 weeks.
There will be a small bounty and we will issue an advisory + CVE as usual.

dashingjaved posted a comment. Mar 30th (8 months ago)

Thanks for the quickly reply...

dashingjaved posted a comment. Apr 4th (8 months ago)

Any update

dashingjaved posted a comment. Apr 7th (8 months ago)

Any updates on the report?

dashingjaved posted a comment. Apr 9th (8 months ago)

Hello security team any update for my advisory???

nickvergessen Nextcloud staff updated the severity from Medium to Low (2.5). Apr 11th (8 months ago)

nickvergessen Nextcloud staff updated the severity from Low (2.5) to Low (1.1). Apr 11th (8 months ago)

Nextcloud rewarded dashingjaved with a $100 bounty. Apr 11th (8 months ago)

nickvergessen Nextcloud staff posted a comment. Apr 11th (8 months ago)

We plan to release public advisories for this issue on 19.04.22. We've added a draft version of the advisory as summary to this report:
https://github.com/nextcloud/security-advisories/security/advisories/GHSA-32j4-9xf3-h2mg

Any bonus update?

extcloud rewarded dashingjaved with a **$100** bounty. Apr 26th (7 months ago)

Congratulations! We have determined this to be eligible for a reward of $100.

Thanks a lot for making the internet a safer place and keep hacking.

dashingjaved posted a comment. Apr 26th (7 months ago)

Thanks for great bounty.

nickvergessen Nextcloud staff requested to disclose this report. Apr 27th (7 months ago)

nickvergessen Nextcloud staff updated CVE reference to **CVE-2022-24885**. Apr 27th (7 months ago)

dashingjaved agreed to disclose this report. Apr 30th (7 months ago)

This report has been disclosed. Apr 30th (7 months ago)