13

Android app does not clear end to end encryption keys

Share:

TIMELINE

rtod submitted a report to Nextcloud. May 8th (2 years ago)

1. userA on serverA sets up end to end encryption on their android device
2. userA has some end to end encrypted data
3. userA removes their account on serverA from their android device (for whatever reason)
4. attacker (evil admin) obtains the device of userA
5. attacker (evil admin) logs in on the account of userA (reset the pw and just log in)
6. attacker (evil admin) can see and access all encrypted files

Impact

While I believe the impact is minimal since you need to obtain the device of the victim.
Once you remove your account all information regarding that account should be removed.

- the keys
- the mnemonic

And certainly when you re-add an account you should be asked to enter your mnemonic!

OT: posted a comment. May 8th (2 years 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. We will reply to your report within 72 hours, usually much faster. For obvious reasons we'd like to ask you to not disclose this issue to any other party.

ullzer changed the status to Triaged. May 10th (2 years ago)

Thanks for the report.
Also here an issue is filled and we'll get back to you once we have more information.

lukasreschkenc posted a comment. May 25th (2 years ago)

The team has looked into this and https://github.com/nextcloud/android/pull/8439 should potentially resolve this.

rtod posted a comment. May 27th (2 years ago)

Yes that looks sane. I guess it is some timeout or some error that might happen. So best to clear those easy things first.

lukasreschkenc posted a comment. Jun 1st (2 years ago)

> Yes that looks sane. I guess it is some timeout or some error that might happen.

That is correct and caused also some issues to reproduce this in our test environments. :)

This should be included in our next release "3.17.0" which will be published probably in June (RC1 is planned for mid June as per https://github.com/nextcloud/android/issues/8353)

lukasreschkenc posted a comment. Jun 1st (2 years ago)

Draft advisory is at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-g5gf-rmhm-wpxw and pending CVE assignment.

Nextcloud rewarded rtod with a $100 bounty. Jun 1st (2 years ago)

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

As an attack requires physical access to the device, we believe the risk is limited here.

Thanks a lot for making the internet a safer place and keep hacking. Please keep in mind that we didn't patch the vulnerability yet, so please do not share this information with any third-parties.

lukasreschkenc updated CVE reference to CVE-2021-32658. Jun 2nd (2 years ago)

lukasreschkenc closed the report and changed the status to Resolved. Jun 2nd (2 years ago)

I have been informed this was fixed in 3.16.1 already. (https://github.com/nextcloud/android/pull/8445)

lukasreschkenc posted a comment. Jun 8th (2 years ago)

The advisory has been published at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-g5gf-rmhm-wpxw

rtod requested to disclose this report. Jun 15th (2 years ago)

lukasreschkenc agreed to disclose this report. Jun 16th (2 years ago)

This report has been disclosed. Jun 16th (2 years ago)