


11 End to end encryption public key is not properly verified on Desktop and Android

Share:     

TIMELINE

 **rtod** submitted a report to [Nextcloud](#). May 8th (2 years ago)
 Since last time when I reported something on multiple platforms you seems to prefer handling it in 1 spot. I now just do one. Let me know if You want me to fill separate for android as well. This issue does not seem to happen on iOS as there a test string is encrypted and decrypted, in short binding the keypair.

So the attack vector results in weird behavior but that seems to be due to random bugs in the end to end encryption implementations (because I also ran into those when just messing around with the end to end encryption). In any case there should be a big error if this happens.

1. userA has an account on serverA
2. End2End encryption is enabled on serverA
3. userA setups device1 and enabled end to end encryption. Stores the nonce. Uploads some data. All is good.
4. Now an attacker obtains access to the server, for sake of argument assume there is an evil Admin.
5. They replace the public key of userA with their own
6. userA now setups device2 7, userA enters the nonce
7. userA uploads more data
8. the evil admin now has access to the uploaded data

Impact

In short it breaks the whole premise of your end to end encryption. An evil admin is able to make the device encrypt to their key.

It is even in the RFC: https://github.com/nextcloud/end_to_end_encryption_rfc/blob/master/RFC.md#further-devices
 "Client checks if private key belongs to previously downloaded public certificate."


Recommendations:

1. the clients should verify that the private key matches with the public key and if not throw a big error

This is especially important because somebody is clearly doing something they are not supposed to if this happens.

 **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.


 **lilizer** changed the status to 🔴 **Triaged**. May 10th (2 years ago)
 Thanks again for your reports :)
 I filled a report internally and we'll get back to you once we have more information.

 **extcloud** rewarded **rtod** with a \$1,500 bounty. May 19th (2 years ago)
 Congratulations! We have determined this to be eligible for a reward of \$1500.

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** posted a comment. May 25th (2 years ago)
 This should potentially be resolved with <https://github.com/nextcloud/desktop/pull/3338> and <https://github.com/nextcloud/android/pull/8438>.

 **rtod** posted a comment. May 27th (2 years ago)
 Looks about right indeed

 **rtod** posted a comment. Jun 23rd (about 1 year ago)
 With those merged I assume this can be closed and disclosed soon.

 **lukasreschkenc** posted a comment. Jun 28th (about 1 year ago)
 I've talked to the product teams here and they told me that they are aiming to release a patched Desktop release at the end of July.

The draft advisories are at:

- [Android](#)
- [Desktop](#)

 **lukasreschkenc** closed the report and changed the status to 🟢 **Resolved**. Aug 3rd (about 1 year ago)
 This should be fixed with 3.3.0 released today.

 **rtod** requested to disclose this report. Aug 24th (about 1 year ago)

 This report has been disclosed. Sep 23rd (about 1 year ago)

