7 End to end encryption folder locking is not properly protected

Share:

TIMELINE

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

I do not see the end_to_end_encryption app listed here. But since you advertise it big on your website and in communication. And the clients (that also support it are covered) I assume this is part of the program as well.

1. userA has end to end encryption setup
2. userB wants to annoy userA
3. userB starts to send curl request like

Code 194 Bytes Wrap lines Copy Download

```
1 curl -u user1:user -X POST https://SERVER/ocs/v2.php/apps/end_to_end_encryption/api/v1/lock/332 -X POST  -H 'OCS-APIREQUEST: true' -H 'user-agent: Mozilla/5
```

Here 332 is a fileid. But it can be any fileid.

4. If userB just keeps looping they can just lock all fileids. Limiting any other user from interacting with their encrypted folders.

Impact

userB in this case can avoid userA from interacting with their encrypted data. Effectively locking them out of adding new data.

Now admitted they do not know which file id the encrypted folder of userA is. But a small script can lock a lot of ids very quickly. And the job to fix this only runs once an hour and clears max 25. So I'm relatively sure that userB has a big advantage here.

Recommendations:

1. While locking there should also be checks (like with unlocking) if the user has access
2. There should be throttling on those endpoints esp if users try to lock things they have no access to

nc-bot: 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.

nldlzer 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.

nldlzer posted a comment. May 10th (2 years ago)

We could verify the issue.
A fix got merged in https://github.com/nextcloud/end_to_end_encryption/pull/237 and backported as well.
We are preparing new releases for this.

Nextcloud rewarded rtod with a $250 bounty. May 10th (2 years ago)

Congratulations! We have determined this to be eligible for a reward of $250.

Thanks a lot for making the internet a safer place and keep hacking. Please do not share this information with any third-parties yet until the advisories are out.

nldlzer closed the report and changed the status to Resolved. May 10th (2 years ago)

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

Please let us know how you'd like to be credited in our official advisory. We require the following information:

- Name / Pseudonym
- Email address (optional)
- Website (optional)
- Company (optional)

rtod posted a comment. May 10th (2 years ago)

Thanks again for the bounty!
Quick fix and seems to do the trick.

Crediting again:

Name: rtod
Email: robottod@protonmail.com

lukasreschkenc changed the scope from nextcloud/server to nextcloud/end_to_end_encryption. May 10th (2 years ago)

lukasreschkenc updated CVE reference to CVE-2021-22906. May 10th (2 years ago)

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

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3829-45wm-ww36

This report has been disclosed. Jun 10th (2 years ago)