165 **User can delete data in shared folders he's not autorized to access**

Share:

TIMELINE

jlord87 submitted a report to Nextcloud. Jul 13th (3 years ago)

Steps to reproduce

1. create a group folder named TEST and share with "admin group" and "test group", marking the advanced permission flag
2. create two folders inside the main share: visible and invisible
3. inside "invisible" folder create a test file (let's say something like "test.txt")
4. set the advanced folder permission to deny everything to "test group" for the "invisible" folder (deny read, deny write, deny share, deny create, deny delete...)
5. log in with test user (member of test group). The invisible folder is not shown, you can only see the visible one. That's great.
6. if you try to create a folder named "invisible" you get an error (that's good too) sync the new external share to your pc (in my case win7 with 2.5.2 client). Only the "visible" folder is synced.
7. create a folder named "temp" and create inside this new folder a new file (lets say "test2.txt"). This folder will be synced online
8. rename temp to invisible
9. the folder gets synced online overwriting the originale "invisible" folder

Expected behaviour

The sync client should keep denying the syncronization of "invisible" folder to the unauthorized users

Actual behaviour

The folder is synced, the original one and all its content (that should be inaccessible to test user) are overwritten and lost

Impact

An "attacker" - that could simply be an user with low privileges - can delete sensitive data that were on purpose hidden to its group.

OT: posted a comment. Jul 13th (3 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.

nickvergessen Nextcloud staff changed the status to **Triaged**. Jul 15th (3 years ago)

nickvergessen Nextcloud staff posted a comment. Jul 15th (3 years ago)

@jlord87 https://github.com/nextcloud/groupfolders/pull/519 should fix the issue, can you confirm?

jlord87 posted a comment. Updated Jul 15th (3 years ago)

I can confirm, the commit e98a80baa44c227e025118e8b1ad36fe7fd6cbd3 solves this bug.
(the client is still not working well, it does not always give errors when renaming the folder to an existing and hidden one. But data are not synced and not deleting the hidden one.)

Good job, thanks

nickvergessen Nextcloud staff closed the report and changed the status to **Resolved**. Mar 11th (3 years ago)

Sorry forgot to close this.

Thanks a lot for your report again. 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)

nickvergessen Nextcloud staff requested to disclose this report. Mar 11th (3 years ago)

Nextcloud rewarded jlord87 with a **$250** bounty. Mar 12th (3 years ago)

nickvergessen Nextcloud staff added weakness "Improper Access Control - Generic". Mar 12th (3 years ago)

jlord87 posted a comment. Mar 14th (3 years ago)

Thank you @nickvergessen, it's an honor to be credited in the official advisory!
you can put this info:
Francesco MORO(sinotto)

Thank you :)

This report has been disclosed. Apr 10th (3 years ago)