3 External storage app saves password for all users in the database

Share:

TIMELINE

alacn1 submitted a report to Nextcloud. May 6th (3 years ago)

External storage (files_external) app save passwords of all users to database table "oc_credentials" even when "Log-in credentials, save in database" option is not used.

It's a security risk that allow password extraction of all users.

A local system admin that has access to database and nextcloud config file could decrypt any user password.

Steps to reproduce

1. Enable app "External storage support" (files_external).
2. Login to nextcloud.
3. User recoverable password will be saved to table "oc_credentials" at "password::logincredentials/credentials".

Expected behaviour

Don't save user password to table "oc_credentials" unless user has a mount with "Log-in credentials, save in database" option.

Actual behaviour

Passwords of all users is saved to table "oc_credentials" when files_external app is enabled.

Tested with

Nextcloud 18.0.4 + External storage 1.9.0
Nextcloud 17.0.5 + External storage 1.8.0

Impact

A local system admin could recover any user password.

OT: posted a comment. May 6th (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.

alacn1 posted a comment. May 6th (3 years ago)

the password is saved by:
apps/files_external/lib/Lib/Auth/Password/LoginCredentials.php:
OCA\Files_External\Lib\Auth\Password\LoginCredentials::authenticate()

there is no check if the user has any mount with "Log-in credentials, save in database" option.

ickvergessen Nextcloud staff posted a comment. May 7th (3 years ago)

I forwarded your report to the correct people.

ewind1991 Nextcloud staff posted a comment. May 8th (3 years ago)

Hello,

you are correct that the credentials should only be saved when a relevant mount is configured.

One issue I can see is that this means that a newly configured storage wont be usable in background jobs/cli for the applicable users until they are active again. Which can lead to unexpected behaviour if an admin tries to do something like running the filescanner for a newly configured mount.

I'll look into the best way to fix this issue and come back once I have some code

nickvergessen Nextcloud staff changed the status to ○ Triaged. May 11th (3 years ago)

ickvergessen Nextcloud staff posted a comment. May 27th (3 years ago)

Pull request: https://github.com/nextcloud/server/pull/21037

extcloud has decided that this report is not eligible for a bounty. May 27th (3 years ago)

The issue is not eligible for a bounty because it was reported publicly before:
https://github.com/nextcloud/server/issues/17439

ickvergessen Nextcloud staff closed the report and changed the status to ○ Resolved. Feb 2nd (2 years ago)

Sorry, forgot to close this.

Thanks a lot for your report again. This has been resolved in our maintenance release from June 2020 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)

alacn1 posted a comment. Feb 2nd (2 years ago)

Name: Anderson Luiz Alves

Email: alacn1@gmail.com

Feb 10th (2 years ago)

nickvergessen Nextcloud staff changed the report title from **files_external app save passwords of all users to database** to **External storage app saves password for all users in the database**.

nickvergessen Nextcloud staff posted a comment. Feb 10th (2 years ago)

Pending SA: https://nextcloud.com/security/advisory/?id=NC-SA-2021-006

Pending CVE: CVE-2020-8296

Scheduled date: 22nd Feb

nickvergessen Nextcloud staff requested to disclose this report. Mar 1st (2 years ago)

nickvergessen Nextcloud staff disclosed this report. Mar 1st (2 years ago)