90

Re-Sharing allows increase of privileges

Share:

TIMELINE

alx_il submitted a report to Nextcloud. Jun 2nd (3 years ago)

- User A shares a file/folder to user B with re-sharing permission, but readonly
- User B shares this file/folder to User C (Needs the shareapi_default_permissions set to 1 (all checkmarks off in admin panel))
- User B can add write permissions for the share to User C (User C may also be anonymous using a link)
- User C gets write access and can edit existing files

Impact

User can get write permission on read-only shared files/folders.

BOT: posted a comment. Jun 2nd (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 ○ Needs more info. Jun 2nd (3 years ago)

Which version of nextcloud were you using? We fixed a case like this earlier this year.

alx_il changed the status to ○ New. Jun 2nd (3 years ago)

18.0.4.2 - see https://github.com/nextcloud/server/issues/21188 for config

alx_il posted a comment. Jun 3rd (3 years ago)

I tried to analyze whats happening: In lib/private/Share20/Manager.php the permissions are calculated. In function generalCreateChecks there is a section
// When it's a reshare use the parent share permissions as maximum
$userMountPointId = $mount->getStorageRootId();
$userMountPoints = $userFolder->getById($userMountPointId);
$userMountPoint = array_shift($userMountPoints);

At this point, $userFolder is the home Folder of User B, $userMountPointId is the Rootid of User A. The resulting Array and $userMountPoint is empty. So the following "$incomingShares = $this->getSharedWith($share->getSharedBy(), Share::SHARE_TYPE_USER, $userMountPoint, -1, 0);" will find ALL Shares from User A to User B and because there is a second share with write permissions here, it will also allow write permissions.

nickvergessen Nextcloud staff posted a comment. Jun 8th (3 years ago)

For me this works until I try to "update" the share permissions.
There I get 404:
Error while updating share Error: "Request failed with status code 404"

But maybe this was fixed in the last release already. Can you try it with 18.0.5 or 18.0.6 (should be published tomorrow)

nickvergessen Nextcloud staff changed the status to ○ Needs more info. Jun 8th (3 years ago)

alx_il changed the status to ○ New. Jun 8th (3 years ago)

Hello,

still working in 18.0.5.1. To get this, there must be a second share from User A to User B with enabled write permissions for the folder. In the Images ("A" is User A, "M" is User B; please do not publish, I did't removed names) the "test2" folder is shared R/W with User B, while "Test" is shared R/O with share permission.

I may try it tomorrow with 18.0.6.

2 attachments:
F859396: Zwischenablage02.png
F859397: Zwischenablage01.png

alx_il posted a comment. Updated Jun 8th (3 years ago)

Sorry, the last message was not clear. The bug is still there in 18.0.5.1. It's still working to enable write permission on a readonly share.
It's required to have a second share with write permission to trigger the bug.

alx_il posted a comment. Jun 9th (3 years ago)

Tested with 18.0.6.0 - bug is still there.

rullzer posted a comment. Jun 9th (3 years ago)

I think we are missing some steps or doing it slightly different.

Could you create a screencast to show all the steps?

Thanks,
--Roeland

F861189: 2020-06-09_21-41-56.mp4

alx_il posted a comment. Updated Jun 9th (3 years ago)

Used the VM to test this with NC 19. It's also in 19.0.0 (same procedure).

ullzer posted a comment. Jun 19th (3 years ago)

Hi,

Thanks.
So weird thing I can see it happen on some folders but not on all.
I'm diving a bit deeper to see what is going on.

Cheers,
--Roeland

ullzer changed the status to Triaged. Jun 19th (3 years ago)

Ok I think I found it.
We are working on a fix.

ullzer posted a comment. Jun 25th (2 years ago)

Hi,

I totally forgot to post it here.
But the fix is in https://github.com/nextcloud/server/pull/21489

Mind to give that a spin?

Cheers,
--Roeland

alx_il posted a comment. Jun 25th (2 years ago)

Hi,

I patched Share20\Manager20.php (I was on the right track in my 3rd posting ;)) and now I can't get higher permissions with resharing. It shows (correctly) "Fehler beim Aktualisieren der Freigabe" in GUI and XHR returns `{"ocs":{"meta":{"status":"failure","statuscode":404,"message":"Kann die Berechtigungen von nicht erh\u00f6hen"},"data":[]}}` if I try to switch on write permissions on the reshared read-only folder.

Thank you for fixing the problem.

Alexander

ullzer posted a comment. Jul 10th (2 years ago)

Hi,

We released the RC of the maintenance releases yesterday. The finals will be next week and they contain the fix for this.

Cheers,
--Roeland

ickvergessen Nextcloud staff closed the report and changed the status to Resolved. Jul 10th (2 years ago)

Thanks a lot for your report again. This has been resolved in our next maintenance 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)

alx_il posted a comment. Jul 10th (2 years ago)

Hello, I have to thank you for fixing the problem so quickly.
You may add my name Dr. Alexander Fleischer and the Company TU Ilmenau if you like.

Have a nice weekend, Alexander

nickvergessen Nextcloud staff updated the severity from Low to Medium (5.5). Jul 29th (2 years ago)

nickvergessen Nextcloud staff added weakness "Improper Privilege Management" and removed weakness "Privilege Escalation". Jul 29th (2 years ago)

ickvergessen Nextcloud staff posted a comment. Jul 29th (2 years ago)

Advisory will be published at: https://nextcloud.com/security/advisory/?id=NC-SA-2020-029
Assigned CVE is: CVE-2020-8202

Publish date is 4 weeks after release of the fixed version:
Release: 16th July
Publish date: 13th August

Since I'm on vacation in those days, I will see if another Nextclouder can publish it, otherwise it will be in the week afterwards.

alx_il agreed to disclose this report. Sep 28th (2 years ago)

This report has been disclosed. Sep 28th (2 years ago)