

15 Missing server side controls when editing the board's sharing permissions per user

Share:     

TIMELINE



warsocks submitted a report to Nextcloud.

Mar 24th (3 ye

Author: Silvia Väli, Clarified Security (<https://www.clarifiedsecurity.com/silvia-vali/>)

Date: 24th of March, 2020

Description:

When the regular user is visiting the Deck view, all created boards are displayed along with the ones that are shared with the user by others. Available functionality within each of the shared boards depends whether the user has received share, manage, edit permissions.

Since the access control rules related to user's permissions have only been applied on the client side and not on the server side, user can specify share/edit/manage permissions to be always true within the response (for example by using a proxy tool) when viewing board information. This way he can gain control over the board he/she could apply the missing edit/manage permissions to him/herself directly from the UI.

Version information:

Nextcloud 18.0.2

Deck 0.8.0 enabled

Pre-requisites as an admin user to follow the vulnerable path:

- create 2 regular users in the next cloud, for example user silvia and user john. Users do not belong to the admin group.
- Install the Deck app (installed version 0.8.0)

To reproduce the vulnerable path:

User: silvia

1. Authenticate as user silvia and select Deck from the menu
2. Create new board -> name it ("board for testing")
3. Add a new stack ("test test")
4. Click on "Show board for details"
5. Add the other user john and only give him Share permission. Uncheck Edit and Manage.

User: john

6. Now authenticate in the application as john -> click Deck from the menu and open the shared board "board for testing". Since the board was only Shared and no permissions were granted, john cannot do much on the board.
7. What john can do however is use a proxy tool such as Burp Suite to modify the response body. When john clicks on the Deck from the menu, following request made:

Code 79 Bytes

[Wrap lines](#) [Copy](#) [Down](#)

```
1 GET /apps/deck/boards HTTP/1.1
2 Host: next.yy.ee
3 ...
4 Connection: close
5 Cookie: ...
```

8. In the response to that request, you can see that john only been given the permission to share which only allows to read the data and not modify it.

Code 535 Bytes

[Wrap lines](#) [Copy](#) [Down](#)

```
1 [{"title":"board for testing",
2  "owner":{"primaryKey":"silvia","uid":"silvia","displayname":"silvia"},"color":"0082c9","archived":false,"labels":[],"acl":[{"participant":{"primaryKey
```

9. john however uses a proxy tool such as Burp Suite and applies via proxy -> options -> Match and replace that every time the following line with permissions is s modify all the options to be equal to true.

Original: `"permissionEdit":false,"permissionShare":true,"permissionManage":false,"owner":false`

Modified: `"permissionEdit":true,"permissionShare":true,"permissionManage":true,"owner":true`

10. If john now refreshes the Deck page and opens the board "board for testing" -> Show board details -> Sharing -> he can add himself the permissions to Edit, Share, Manage to take over the board which was initially only shared with him.

Impact

Attacker would achieve control over the board and its data/attachment uploads etc.

1 attachment:

F758412: [Report_SILVIA_V_LI_24.03.2020.pdf](#)



OT: posted a comment.


Mar 24th (3 ye

you do not disclose this issue to any other party.


 Nextcloud staff posted a comment. Mar 24th (3 ye
Thanks for the report, I will forward this to the Deck Developers


 posted a comment. Mar 24th (3 ye
Thank you for a quick response. Will look forward to receiving some feedback from the Deck Developers then.

 Nextcloud staff updated the severity from Critical (9.6) to High (7.7). Mar 30th (3 ye

 Nextcloud staff changed the status to Triaged. Mar 30th (3 ye
Hello,


thanks again for your report. I could now reproduce the issue that users could extend their permissions when they have sharing permissions. We are now working fix so that updating permissions will always be limited to the own permission level.


 posted a comment. Apr 1st (3 ye
Glad you managed to reproduce it well. If there is anyway I could help you, or any further questions, fire away.


 Nextcloud staff posted a comment. Apr 6th (3 ye
Hi,

just a quick update. We have a fix for the issue prepared at <https://github.com/nextcloud/deck/pull/1653/files#diff-e448525c1380ca5a2202113c6f85e094> and will prepare new releases of the deck app once that has been reviewed.

 posted a comment. Apr 8th (3 ye
Thank you for the update, will review.


 posted a comment. Apr 8th (3 ye
Just to make sure we both understand how the functionality is intended to behave now after the fix, could you please clarify this part of your sentence "...updating permissions will always be limited to the own permission level" with an example please.

 posted a comment. Apr 9th (3 ye
In v0.8.2 I was not able to replicate the same vulnerability anymore and when trying to elevate my permissions always received the response HTTP/1.1 403 Forbidden. So from my side, it can be counted as fixed.


 Nextcloud staff closed the report and changed the status to Resolved. Apr 9th (3 ye
Thanks a lot for your report again. This has been resolved in our latest 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)


 posted a comment. Apr 9th (3 ye
Below you can find my information. I would also like to know if a CVE be requested for the vulnerability and is my finding eligible for a bounty? :)

Name: Silvia Väli
E-mail: silvia@clarifiedsecurity.com
Website: <https://www.clarifiedsecurity.com/silvia-vali/>
Company: Clarified Security

 Nextcloud rewarded warsocks with a \$100 bonus. Apr 9th (3 ye
While the app is not in scope for a bounty, we decided to give you a \$100 bonus.

 Nextcloud staff posted a comment. Apr 9th (3 ye
All our security issues will be published as a Security Advisory on our website and then be requested a CVE after ~4 weeks

 posted a comment. Apr 14th (3 ye
Thank you so much for assigning a bounty @Nextcloud, @nickvergessen and the Deck developers and a Happy Easter!

 posted a comment. May 18th (3 ye
Hello, you mentioned I would be credited in your official advisory. I have not managed to find a reference to it, could you kindly direct me to it please?

 Nextcloud staff updated the severity from High (7.7) to High (7.3). Jun 8th (3 ye

 Nextcloud staff changed the scope from nextcloud/3rdparty to nextcloud/server. Jun 8th (3 ye

 Nextcloud staff posted a comment. Jun 8th (3 ye

we got CVE-2020-0106 assigned for the issue which will be published soon too.



nickvergessen
Published

Nextcloud staff

posted a comment.



nickvergessen

Nextcloud staff

requested to disclose this report.

Jun 15th (3 ye

Sep 28th (2 ye

