# New users can read all Nextcloud Deck data from previous user with same username

0

Share:

TIMELINE

stefanniedermann submitted a report to Nextcloud. May 25th (3 years ago)

First of all: Sorry, i know there is no scope "Deck" but both Joas and Jus pointed me to hackerone to report this security issue.

1. As an administrator create Nextcloud account "test"
2. Log in as "test"
3. Go to Deck app and create some boards, stacks and cards with personal or confidential stuff.
4. As an administrator delete Nextcloud account "test"
5. As an administrator create new Nextcloud account "test" (password doesn't need to match)
6. Log in as "test" (This might be a completely other human than in step 2!)
7. Go to Deck app and see all the secret stuff from the previous user

### Impact

Attacker is able to see confidential or private data from previous users with the same user name.

Since the private data of the users is sacred, it is a no-go that the data isn't hard deleted form the database when the user account gets deleted, but it is even worse that another user with the same username can read all the stuff (without any effort to restore data).

nc-bot: posted a comment. May 25th (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.

juliushaertl Nextcloud staff changed the status to Triaged. May 26th (3 years ago)

juliushaertl Nextcloud staff posted a comment. May 26th (3 years ago)

Thanks for the report. I can indeed reproduce this and we are working on a fix. I'll keep you updated.

juliushaertl Nextcloud staff posted a comment. Jun 2nd (3 years ago)

A quick update, we have a fix waiting for review in https://github.com/nextcloud/deck/pull/1976

nickvergessen Nextcloud staff updated the severity to Low. Jun 10th (3 years ago)

nickvergessen Nextcloud staff closed the report and changed the status to Resolved. Jun 10th (3 years ago)

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)

nc-bot has decided that this report is not eligible for a bounty. Jun 10th (3 years ago)

Since deck is not "in scope" for bounties and this is also only a hardening and not actively abusable by normal users we decided it's not eligible for a bounty.

nickvergessen Nextcloud staff requested to disclose this report. Jan 15th (2 years ago)

stefanniedermann posted a comment. Feb 9th (2 years ago)

@nickvergessen

**Code** 93 Bytes Wrap lines Copy Download

```
1 Stefan Niedermann
2 info@niedermann.it
3 https://www.niedermann.it
4 Niedermann IT-Dienstleistungen
```

nickvergessen Nextcloud staff added weakness "Insecure Direct Object Reference (IDOR)". Feb 10th (2 years ago)

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

Pending SA: https://nextcloud.com/security/advisory/?id=NC-SA-2021-007
Pending CVE: CVE-2020-8297

Scheduled date: 22nd Feb

This report has been disclosed. Feb 14th (2 years ago)