


15 Access control missing while viewing the attachments in the "All boards"

Share:     

TIMELINE

 dpx01 submitted a report to [Nextcloud](#). Jul 6th (2 ye
The vulnerability lies in the "view attachment" of the tasks . When a user uploads the file to the Task, the attachment is given a numeric number and is increased +1 further uploads. It is easy for any user to view and download all the files uploaded to the tasks by any user. The access is not controlled with the session or csrf token.

Steps to Reproduce:

1. Connect to the server login with user A and visit the webpage. I used the provider "us.cloudamo.com"
2. Visit <https://us.cloudamo.com/apps/deck> and create a task.
3. Upload any file to the attachments and capture the request. The request will look like "<https://us.cloudamo.com/apps/deck/cards/8420/attachment/30>" where 30 is the ID of the uploaded attachment.
4. Login with user B and access the URL and you should be able to view the attachment of user A.
5. Since the attachment IDs are numerical number with poor entropy can be easily brute-forced and one can get all the uploaded attachments by all the users of particular provider.

Impact

Unauthorized user can view and download the files of other users. This may leak the sensitive information of users.


2 attachments:
F896401: [IDOR_01.png](#)
F896402: [IDOR_02.png](#)

 YOT: posted a comment. Jul 6th (2 ye
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.


 dpx01 posted a comment. Jul 6th (2 ye
Similarly, the attachments can also be deleted using same IDOR vulnerability. Attaching the screenshot for delete attachment of another user (pendev) using divy.er@gmail.com account.

1 attachment:
F897208: [delete_attachment_IDOR.png](#)

 [juliushaertl](#) Nextcloud staff posted a comment. Jul 7th (2 ye
Thanks a lot for your report again. We could not reproduce the issue you are describing with the latest release of Deck. Could you report which version you are running? Can you further verify that the board that contains the attachment is not shared to the user B or a group that the user is part of?

For users without read access to a board the attachment url should return a 403 response no matter if the attachment exists or if the user just doesn't have access. We don't see any attack vector based on the incremental integer id.


 [juliushaertl](#) Nextcloud staff changed the status to ● Needs more info. Jul 7th (2 ye

 dpx01 changed the status to ● New. Jul 7th (2 ye
[@juliushaertl](#) as mentioned earlier, I am using the hosting service provider "us.cloudamo.com" not sure which version I am running of. I could not find a version on the portal. Please help me to identify the same.
I can confirm that I have not added another user B in the board group.

I have attached a video to show the successful fetching of the attachments uploaded by any user. Please have a look. Hope this helps.

Please let me know, if further information is required.

1 attachment:
F897650: [NextCloud_Deck_IDOR.mp4](#)































 [juliushaertl](#) Nextcloud staff posted a comment. Jul 7th (2 ye
Thanks a lot for the video. I could now indeed reproduce the issue when keeping the card id in the url that is valid for the user. We will look into this and keep you updated.

 [nickvergessen](#) Nextcloud staff changed the status to ● Triaged. Jul 7th (2 ye

 dpx01 posted a comment. Jul 7th (2 ye
Glad that you are able to reproduce and thanks for the triage.

You may want to modify the CVSS score, as the files are not only fetched but also gets deleted, that impacts the integrity and availability.

 dpx01 posted a comment. Aug 9th (2 ye

<p>    updated the severity from <u>High (7.5)</u> to <u>Medium (6.5)</u>. </p>	Aug 12th (2 ye
<p>   posted a comment. Hello, sorry for the delay and for the missing update. We have pushed out a fix for this issue with the latest patch update v1.0.5 of deck. </p>	Aug 12th (2 ye
<p>    changed the status to Triaged. </p>	Aug 12th (2 ye
<p>  posted a comment. Thanks for the response @juliushaertl I see the attachments are protected now and responds with 403 "Permission denied". </p>	Aug 13th (2 ye
<p>  posted a comment. Just curious on severity change. Since the user was able to delete file as well shouldn't it impact the integrity and availability? </p>	Aug 13th (2 ye
<p>  posted a comment. @juliushaertl Any update please? If there is no change, the issue is verified and fixed now. This can be closed unless there is any action is pending from my end. </p>	Aug 17th (2 ye
<p>   closed the report and changed the status to Resolved. 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: <ul style="list-style-type: none"> • Name / Pseudonym • Email address (optional) • Website (optional) • Company (optional) </p>	Aug 17th (2 ye
<p>  posted a comment. Thanks, But surprising, why isn't this reported eligible for bounty? Can you please help to make me understand this. </p>	Aug 17th (2 ye
<p>   posted a comment. We are still discussing things here. Deck is currently not in scope, but we might assign a bonus nevertheless. However this shall not delay publication of the finding unnecessarily. </p>	Aug 17th (2 ye
<p>  Nextcloud rewarded dpx01 with a \$150 bonus. The deck app is not in scope. However we did decide to award you a bonus. </p>	Aug 17th (2 ye
<p>  posted a comment. Understood. Thanks appreciated. Please use below information for security advisory. Name: Divyesh Prajapati </p>	Aug 17th (2 ye
<p>  Aug 17th (2 years ago)   changed the report title from Access control missing while viewing the attachments in the "All boards", leads to Insecure Direct Object Reference to Access control missing while viewing the attachments in the "All boards". </p>	
<p>   posted a comment. Requested CVE: CVE-2020-8235 Advisory will be published at https://nextcloud.com/security/advisory/?id=NC-SA-2020-036 </p>	Aug 17th (2 ye
<p>  posted a comment. Thanks for the update. And honored to be in advisory. Appreciate. </p>	Aug 18th (2 ye
<p>    requested to disclose this report. </p>	Sep 28th (2 ye
<p>   agreed to disclose this report. </p>	Sep 29th (2 ye
<p>  This report has been disclosed. </p>	Sep 29th (2 ye