

14

When sharing a Deck card in conversation the metaData can be manipulated to open arbitrary URL

Share:     

SUMMARY BY NEXTCLOUD



Summary:

This report is similar to [#1337178](#)

In Nextcloud Deck a user can post their decks in to a conversation via nextcloud talk. The `link` in `metaData` can be manipulated to point to a another URL.

Steps To Reproduce:

- 0.) Setup burpsuite to proxy
- 1.) Go to Nextcloud Deck and pick a board
- 2.) Pick any cards, It will open a page on the Top Right there is a 3 dots (toggle menu i think) Click it press `Post to a Conversation`
- 3.) Post the card to any conversation (if you see nothing, Start a conversation to a seperate account)
- 4.) Go to burpsuite and find the request it should be like the request below

Code 319 Bytes

```
1 POST /ocs/v2.php/apps/spreed/api/v1/chat/9wdc7nta/share HTTP/2
2
3 {"objectType":"deck-card","objectId":"9","metaData":{"id":"9","name":"Examp
```

- 5.) Send the request to repeater and modify the link and send the request

[Show more](#)


















TIMELINE



[culhu](#) submitted a report to [Nextcloud](#).

Oct 5th (about 1 year ago)



-  [lukasreschkenc](#) posted a comment. Oct 26th (about 1 year ago)
-  [ctulhu](#) posted a comment. Nov 23rd (about 1 year ago)
-  [ctulhu](#) posted a comment. Dec 11th (12 months ago)
-  [nickvergessen](#) Nextcloud staff posted a comment. Dec 14th (12 months ago)
-  [nickvergessen](#) Nextcloud staff closed the report and changed the status to Resolved. Dec 14th (12 months ago)
-  [ctulhu](#) posted a comment. Updated Dec 14th (12 months ago)
-  [ctulhu](#) posted a comment. Feb 11th (10 months ago)
-  [Nextcloud](#) rewarded [ctulhu](#) with a \$100 bounty. Feb 11th (10 months ago)
-  [ctulhu](#) posted a comment. Feb 12th (10 months ago)
-  [nickvergessen](#) Nextcloud staff requested to disclose this report. Feb 15th (9 months ago)
-  [ctulhu](#) agreed to disclose this report. Feb 15th (9 months ago)
-  This report has been disclosed. Feb 15th (9 months ago)
-  [ctulhu](#) posted a comment. Mar 8th (9 months ago)
-  [nickvergessen](#) Nextcloud staff posted a comment. Mar 21st (8 months ago)
-  [nickvergessen](#) Nextcloud staff updated the severity from Medium to Medium (5.0). Apr 5th (8 months ago)
-  [nickvergessen](#) Nextcloud staff posted a comment. Apr 5th (8 months ago)
-  [nickvergessen](#) Nextcloud staff updated CVE reference to [CVE-2022-24887](#). Apr 27th (7 months ago)

