

8

## Share recipient can modify a share's expiration date

Share:     

### TIMELINE



icewater submitted a report to Nextcloud.

Nov 20th (4 ye

#### Vulnerable URL

`http://[server]/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares/[share ID number]`

#### Summary

Nextcloud users can set expiration dates on documents they share with others. However, the function to update a share does not appear to properly validate the requester is the owner when changing a share's expiration date. A user could exploit the vulnerability to extend the expiration date of a file shared with them.

The vulnerable parameter appears to be the share ID number at the end of the request URL. Sample request:

```
PUT /nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares/74 HTTP/1.1
OCS-APIREQUEST: true
Authorization: Basic
anJIYWN0Zl6d0xzVU5vVnpDZDFsNGpkdmlxZnFtOWIGUHpWbDRmWkNHTDdTMUtxRmI3R3M1ZlFhc1FVUXNOV2tvY3gwcUVmbllnNmdBMVJR
User-Agent: Mozilla/5.0 (Android) ownCloud-android/3.3.2
Host: 192.168.1.22
Cookie: nc_sameSiteCookielax=true; nc_sameSiteCookiestrict=true;
oc_sessionPassphrase=O5dbusaO3KwFs6e2P4ew7oE99UIUYbbpGa8ZwH01u6gHsvVjPiXfj362cyMkq4XNlIbYCqHESynLeG9VCWUDHHM%2B%2FHeitr910brH
Tc5NnBy7g0JoY1uj1aY9KRQf7; oc0xkd3iidt=fc7vbute5s5efftq2k9af9op0
Content-Length: 21
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Connection: close

expireDate=2018-11-25
```

#### Reproduction

Pre-requisites: a Nextcloud server with a couple of test users, a browser setup to go through a proxy like Burp.

- Go to Burp, click the "Proxy" tab, click the "Intercept" subtab, and click "Intercept is On" to toggle interception off (if it's not already off)
- Login to Nextcloud with a test user
- Share a file with another user. Set an expiration date, for example 17-05-2019
- Go to Burp, click the "Proxy" tab, click the "HTTP history" subtab, scroll down the list and find the call to the vulnerable URL. Note the value for the share ID (the integer at the end of the URL)
- Logout of Nextcloud
- Login to Nextcloud as the user you just shared the file with

At this point, we need to submit the vulnerable request as this second user. However, the vulnerable URL uses the PUT method so copy/pasting into a browser isn't really feasible. One way is to use a legitimate request as a "template" and insert the share ID of the file shared with us.

- As the second user, open a file's sharing dialog and share it with any user
- Go to Burp -> Proxy -> Intercept and toggle interception on
- Go back to the browser and set an expiration date such as 17-05-2020
- Burp should stall the request for viewing. The request should be to the vulnerable URL; if it isn't, click "Forward" until the vulnerable URL appears
- At the end of the URL, change the share ID number to the share ID noted earlier (the share ID of the file shared with the current user by the first user)
- Forward the request (or toggle interception off, either works)
- Logout and log back in as the first user. Navigate to the shared file and look at the expiration date. It should be 17-05-2020, demonstrating the share recipient extended their access to the file by a year.

#### Screenshots

1\_request - vulnerable request as seen in Burp.

#### Impact

#### Impact/Notes

If someone shares a static file with another user, the vulnerability is less of an issue. The user granted access could download an offline copy and refer to it after share access expires.

Where this issue becomes more concerning is with "living" files that an individual might frequently edit, like a spreadsheet. A share recipient could extend their access and continue to view updated file contents until someone noticed the share instance was still in place.

This does not appear to affect groups; i.e. if a group is the recipient of a share I have not been able to successfully invoke this vulnerability as a group member.

If I can provide any further information or help with proof of concept please let me know. Thanks!

1 attachment:

F378094: 1\_request.png



YOT: posted a comment.

Nov 20th (4 ye

you do not disclose this issue to any other party.



rullzer posted a comment.

Hi @icewater,

Thanks for your report.

I'll try to reproduce this and get back to you.

Cheers,

--Roeland

Nov 20th (4 ye



rullzer changed the status to Triaged.

Hi,

I could reproduce this.

A fix is on the way.

Cheers,

--Roeland

Nov 20th (4 ye



icewater posted a comment.


Awesome, thanks for the quick reply!

Nov 22nd (4 ye



rullzer updated the severity from Low to Medium (4,3).

Nov 29th (4 ye



rullzer posted a comment.

Hi,


This is fixed in <https://github.com/nextcloud/server/pull/12544>

It is already shipped in the latest maintenance releases. Could you verify this?

Cheers,

--Roeland

Dec 4th (4 ye



icewater posted a comment.

Hi Roeland, I updated my test instance and can no longer reproduce this issue.

Thanks,

Dec 4th (4 ye




rullzer posted a comment.

Perfect. Thanks for testing.

I'll soonish (probably in the new year) publish the advisories.

Dec 18th (4 ye




nextcloud rewarded icewater with a \$100 bounty.

Congratulations! We have determined this to be eligible for a reward of \$100.

Thanks a lot for making the internet a safer place and keep hacking. Please keep in mind that we didn't release the advisories yet, so please do not share this information with any third-parties.

Dec 18th (4 ye



icewater posted a comment.


Sounds good, thanks for the update

Dec 23rd (4 ye



rullzer added weakness "Improper Access Control - Generic" and removed weakness "Insecure Direct Object Reference (IDOR)".

Jan 8th (4 ye



rullzer 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:

- Name / Pseudonym
- Email address (optional)
- Website (optional)
- Company (optional)

Jan 8th (4 ye




icewater posted a comment.

Thanks! I can be credited as:

Name: Carl Pearson

Website: cp270.wordpress.com

Jan 10th (4 ye



rullzer posted a comment.

Sorry for the delay here. I just wrote the advisory and a CVE will be requested. This will be disclosed ASAP

Apr 11th (4 ye



icewater posted a comment.


No worries, thanks for following up

May 6th (4 ye




nickvergessen (Nextcloud staff) requested to disclose this report.

Jan 31st (3 ye

 icewater agreed to disclose this report.  
No problem, thanks for the followup

Jan 31st (3 ye

 This report has been disclosed

1 - 10 of 10