


53 Default Nextcloud Server and Android Client leak sharee searches to Nextcloud

Share:     

TIMELINE

- 

rtod submitted a report to [Nextcloud](#). Apr 18th (2 ye

On a clean Nextcloud setup the functionality "Search global and public address book for users" is enabled.

Now when searching for a sharee to share with. The lookup parameter is not passed to the server. Resulting in https://github.com/nextcloud/server/blob/master/apps/files_sharing/lib/Controller/ShareesApiController.php#L144


the lookup being true. So the lookup server of Nextcloud will be searched by default.

It seems that the lookup server is down now. But this seems to be an error I assume?

Impact


Anybody sharing trough the android app. Leaks their sharee searches to the Nextcloud lookup server.

Now the server can only see the origin Nextcloud server (or rather the IP of that). Still. This should not be leaked by default.

On the web and desktop there is first a local search. And only if the user explicitly presses the search globally the lookup server is queried. (to be fair this could also more clear that it actually sends data to other systems)
- 

OT: posted a comment. Apr 18th (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 you to not disclose this issue to any other party.
- 

Wilzer posted a comment. Apr 19th (2 ye


Good morning,

Thanks for your report. We'll try to validate it and get back to you.

Cheers,


--Roeland
- 

lukasreschkenc changed the status to Triaged. Apr 19th (2 ye

We have opened a ticket for the product team and will get back to you once we have updates.
- 


Nextcloud rewarded rtod with a \$750 bounty. May 1st (2 ye

Congratulations! We have determined this to be eligible for a reward of \$750. This is a combined reward also for the iOS and Deck app with the same issue.


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

rtod posted a comment. May 1st (2 ye

Again, thanks!

I assume that the Android patch will also soon be released?
- 


lukasreschkenc posted a comment. May 3rd (2 ye

The Android team told us they are aiming to release a patch for this issue this week. I'll verify this with them to confirm.
- 

Wilzer closed the report and changed the status to Resolved. May 10th (2 ye

Thanks a lot for your report again. This has been resolved in our latest android 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)
- 


rtod posted a comment. May 10th (2 ye


Thanks again for the bounty!

Quick fix and seems to do the trick.

Crediting again:

Name: rtod

Email: robbottod@protonmail.com
- 

lukasreschkenc updated CVE reference to [CVE-2021-22905](#). May 10th (2 ye
- 

lukasreschkenc requested to disclose this report. Jun 1st (2 ye

⊖ This report has been disclosed.

Jun 15th (2 ye

