5

Default Nextcloud server config and iOS Nextcloud client leak sharee searches to Nextcloud

Share:

TIMELINE

rtod submitted a report to Nextcloud. Apr 18th (2 years ago)

In short this is the same as https://hackerone.com/reports/1167916 but then for iOS so please forgive the copy paste

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.

Impact

Anybody sharing trough the android app. Leaks their sharee searches to the Nextcloud lookup server.
Now the server can 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 be more clear that it actually sends data to other systems)

BOT: posted a comment. Apr 18th (2 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.

ullzer posted a comment. Apr 19th (2 years ago)

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 years ago)

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

extcloud has decided that this report is not eligible for a bounty. Apr 26th (2 years ago)

We'll bundle the bounty here as well with #1167916.

ullzer posted a comment. Apr 26th (2 years ago)

This has been resolved in the latest release to the appstore

ullzer closed the report and changed the status to ○ Resolved. Apr 26th (2 years ago)

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

This will be disclosed together with the deck/android one.

rtod requested to disclose this report. May 1st (2 years ago)

Please use (again)

Name: rtod
Email: robottod@protonmail.com

I get that this will get disclosed together with the android and deck one.

lukasreschkenc updated CVE reference to CVE-2021-22912. May 26th (2 years ago)

This report has been disclosed. May 31st (2 years ago)

lukasreschkenc posted a comment. Jun 1st (2 years ago)

Advisory at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-m7w4-cvjr-76mh