42 **SSL certificate not validated when registering with a provider**

Share:

TIMELINE

icewater submitted a report to Nextcloud. Jun 19th (2 years ago)

### Description

When running the desktop client for the first time, users can click the "Register with a provider" button to sign up for a Nextcloud account with a Nextcloud cloud provider. Clicking "Register..." opens a web page in a Nextcloud desktop client window with content from https://nextcloud.com/register.

However, the desktop client doesn't appear to validate the SSL certificate for nextcloud.com. An attacker between the user and nextcloud.com could replace the certificate with their own invalid cert and conduct a man in the middle attack. The attacker could control the page content displayed to the user.

This appears to affect Windows and Linux Nextcloud desktop clients. I don't have a Mac so haven't tested the Mac client.

### Reproduction

If you have Burp HTTP proxy, set the Nextcloud client to proxy traffic through Burp. Click "Register with a provider"; Burp should receive the request. This demonstrates vulnerability presence because the Nextcloud client should alert on Burp's self signed certificate, but doesn't.

Otherwise, I wrote a quick python script to demonstrate the vulnerability. You will need at least 1 Linux machine to run the script on. You can run Nextcloud desktop on it too or on another device.

1. Download the attached nc_desktop_mitm.py, nc_key.pem (private key), and nc_cert.pem (public cert) files to a Linux machine.
2. Start the nc_desktop_mitm.py script. The option -k specifies the private key file and -c specifices the public cert file. Sudo is required because we bind to port 443: sudo python3 nc_desktop_mitm.py -k nc_key.pem -c nc_cert.pem
3. Note the IP address of the machine running the script.
4. Now we need to mimic what an attacker could accomplish through ARP poisoning, DNS spoofing, or by controlling a router between the victim and nextcloud.com. However, MiTM techniques like these are tedious to setup, so we'll cheat... Open the hosts file on the device where you are running Nextcloud desktop.
5. Add an entry to point nextcloud.com to the IP of the machine running the script. Save and close the hosts file.
6. Open Nextcloud desktop client and click "Register with a provider".
7. The Nextcloud client displays my custom proof of concept page, indicating the client trusted the invalid cert.

I've attached a screenshot of what the Nextcloud client should show after clicking "Register with a provider" if the reproduction steps worked.

Tested Nextcloud desktop client version 2.6.4stable (build 20200303) on Ubuntu 18.04 and Windows 10. If I can provide further information please let me know. Thanks!

### Impact

An attacker can serve untrusted HTML, Javascript, etc in the trusted context of the desktop client. A typical user is likely inclined to trust what is shown to them in the Nextcloud app compared to a web browser page; they won't even know it's web content necessarily and may assume it's native to the Nextcloud client.

A likely attack vector would be to replace the content with a fake login page and try to get the user to login. If the user clicks "Register with a provider", a window asking them to "Sign in with Google/Facebook/Apple to access your new Nextcloud account!" or similar might net the attacker something useful. Such an attack would probably have a decent success rate given the circumstances.

If an attacker just passively eavesdrops on the user's traffic, near as I can tell the attacker can collect the user's email as it gets POSTed to nextcloud.com during the registration process. A user's email is private, but the usefulness to an attacker seems limited without other associated user information.

4 attachments:
**F875078:** nc_cert.pem
**F875079:** nc_key.pem
**F875080:** nc_desktop_mitm.py
**F875081:** successful_exploit.png

NOT: posted a comment. Jun 19th (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**. Jun 29th (2 years ago)

The issue has been confirmed by our desktop team.

icewater posted a comment. Jan 11th (2 years ago)

Hello Nextcloud, hope your day is going well. I was wondering if there is perhaps an update on this issue? Thanks!

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

Our engineering team is looking into this at the moment.

lukasreschkenc closed the report and changed the status to **Resolved**. Feb 16th (2 years ago)

Thanks a lot for your report again. This will be resolved in our next releases and we're working on the advisories at the moment.
https://github.com/nextcloud/desktop/pull/2926 contains the related patch.

Please let us know how you'd like to be credited in our official advisory. We require the following information:

- Name / Pseudonym

icewater posted a comment. Feb 16th (2 years ago)

Great, thank you! I can be credited as:
Name: Carl Pearson
Email: icewater@wearehackerone.com
Website: https://cpearson.icu/

lukasreschkenc updated CVE reference to **CVE-2021-22895**. Apr 26th (2 years ago)

extcloud rewarded icewater with a **$300** bounty. May 1st (2 years ago)

We have just requested a CVE identifier for this and should be able to publish the advisories soon. Apologies for the delay.

In the mean time, we have assigned a bounty of $300 for this. There is significant user interaction required in a non default flow, which reduced the monetary award.

Thanks again for your report. Much appreciated! :)

icewater posted a comment. May 2nd (2 years ago)

No problem, thank you Nextcloud! Understood, the bug had limited direct impact. Have a great summer

lukasreschkenc requested to disclose this report. Jun 1st (2 years ago)

Thanks again for your report. The advisory can be found at https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qpgp-vf4p-wcw5 and this has been assigned CVE-2021-22895.

icewater agreed to disclose this report. Jun 1st (2 years ago)

This report has been disclosed. Jun 1st (2 years ago)