3 PIN for passwordless WebAuthn is asked for but not verified

Share:

TIMELINE

dschuermann submitted a report to Nextcloud. Jul 15th (2 years ago)

Nextcloud introduced WebAuthn passwordless authentication with version 19. As far as we understand, you assume that your implementation provide two-factor authentication:

"The server asking for authentication can request verification of multiple factors, so that a configured key requires the user to not just plug it in but also enter a PIN or scan a finger print." (see https://www.nitrokey.com/news/2020/what-passwordless-world-looks)

We found the same issue like in Microsoft's implementation: userVerification is not set and the UV flag is not checked on the server. Thus, even though a FIDO2 key with a PIN is added in a user account, the PIN is not required to log in.

The full description is available in our unlisted blog post at: https://hwsecurity.dev/2020/06/webauthn-pin-bypass/

Impact

We have a nice video in our blog post: https://hwsecurity.dev/2020/06/webauthn-pin-bypass/

An attacker could log into the victims account without a PIN by sneaking up on the victim and using the security hardware over NFC.

[bot]: posted a comment. Jul 15th (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.

jullzer posted a comment. Jul 15th (2 years ago)

Hi @dschuermann,

No webauthn in Nextcloud is right now not a replacement for 2FA right now.
That is why it also still will pass you trough your setup 2FA. Hence you can login with webauthN and TOTP etc.

Allowing webauthn to also act as second factor authentication is still on the list. But you are right this would require actually requiring the second factor (be it PIN, biometric etc) to be entered.

However, I will check if the library actually gives us back that a PIN is set and hence if we can from then on require it.

Cheers,
--Roeland

dschuermann posted a comment. Updated Jul 15th (2 years ago)

Just to validate that we are on the same page:

So what I can do right now:
Log into Nextcloud with username and security key only by clicking on "Log in with a device".
No password was required. When using our tampermonkey script there is also no PIN required.

This is unexpected, since when adding the security key, Chrome asks the user to set a PIN.

This also goes against what is written in Nitrokey's blog post, I quoted earlier.

You can easily set userVerification = "required" and check the UV flag in the signature returned from the security key. Details are in our post.

jullzer posted a comment. Jul 15th (2 years ago)

Hi,

So of course my fido2 test key that actually supports me setting the pin is a bit broken.
But I'll get a new one and get back to you.

Cheers,
--Roeland

jullzer posted a comment. Jul 15th (2 years ago)

> Log into Nextcloud with username and security key only by clicking on "Log in with a device".
> No password was required. When using our tampermonkey script there is also no PIN required.

That is just because you are directly logged in. Wait 15 minutes and you will have to enter your password.

> This also goes against what is written in Nitrokey's blog post, I quoted earlier.

Let me reach out to them

> You can easily set userVerification = "required" and check the UV flag in the signature returned from the security key. Details are in our post.

Yes. However this is not what we want. Since it is currently not meant as a 2FA repalcement. So you can also use it without user verification with your old keys. And then use TOTP for the second factor.

However like I said. I'll get back to you once I have a real working FIDO2 key again ;)

dschuermann posted a comment. Jul 15th (2 years ago)
Please put me in CC when reaching out to Jan Suhr. We know each other :)

ullzer posted a comment. Jul 15th (2 years ago)
Sure. What is your e-mail?

dschuermann posted a comment. Jul 15th (2 years ago)
dominik@cotech.de

ullzer posted a comment. Jul 15th (2 years ago)
Mail send.
and a new key is on its way.

In any case thanks for reporting it. I'll see if we have time in the 20 cycle still to tackle it. Including really allowing it to also act as primary+secondary factor. But this might get very tight.

dschuermann posted a comment. Updated Jul 15th (2 years ago)
What do you mean with "20 cycle"?

Do you have a recommendation regarding the disclosure of the blog post? I am also open to re-phrasing parts of it.

dschuermann posted a comment. Jul 15th (2 years ago)
I thought about our discussion:
If Nextcloud's implementation does not verify the UV flag in the signature's authData, you should not ask the user for the PIN, so a "quick fix" is to set userVerification = "discouraged".
This way the user is not asked for a PIN; and thus the threat model is as expected.

Also see Chrome currently emits a warning on Nextcloud's web app:
https://chromium.googlesource.com/chromium/src/+/master/content/browser/webauth/uv_preferred.md

ullzer posted a comment. Jul 15th (2 years ago)
> What do you mean with "20 cycle"?

Ah Nextcloud 20. I meant the general really using a 2FA provider.

> If Nextcloud's implementation does not verify the UV flag in the signature's authData, you should not ask the user for the PIN, so a "quick fix" is to set userVerification = "discouraged".
> This way the user is not asked for a PIN; and thus the threat model is as expected.

Ah thanks. Yes I guess that is the easiest for now. I actually found my notes and have it in there to not ask for this. But I think it slipped trough when testing.

> Do you have a recommendation regarding the disclosure of the blog post? I am also open to re-phrasing parts of it.

Maybe something with

- Similar issues occurred on Nextcloud 19.0.0 and 19.0.1
- However Nextcloud still had 2FA in place after logging in with webauthn
- You have been in contact with Nextcloud to improve this

It is a bit infortunate that we just packaged up the maintenance releases. But I'll make sure this gets attention in the next round (in 6 weeks that is).

Cheers,
--Roeland

dschuermann posted a comment. Jul 20th (2 years ago)
Hi Roeland,

I updated the Nextcloud section: https://hwsecurity.dev/2020/06/webauthn-pin-bypass/#nextcloud-19

I still don't get this point: "However Nextcloud still had 2FA in place after logging in with webauthn"

I didn't get any password prompt when using the passwordless login, not even after 15 minutes.

What's the timeline of the disclosure? Do you consider it a vulnerability? If not, we would publish the blog post.

Cheers
Dominik

ullzer posted a comment. Jul 20th (2 years ago)
Hi Dominik,

> "However Nextcloud still had 2FA in place after logging in with webauthn"

What I mean is that if you have 2FA setup. You will still be prompted for this.

> I didn't get any password prompt when using the passwordless login, not even after 15 minutes.

You should after you try to do some things. Like adding an app password or a webauthn device.

so:

1. Log in
2. Wait 20 minutes (just to be safe)

We don't really consider this a vulnerability more hardening. As it was right now not meant to replace 2FA. More to replace passwords.

I'll go over your revised blog tomorrow.

Thanks for the quick responses and suggestions!

Cheers,
--Roeland

dschuermann posted a comment. Jul 20th (2 years ago)
Thanks, I updated the post again.

I have no more questions :)

Please give me your okay as soon as possible and we will publish the post.

nickvergessen Nextcloud staff changed the status to ○ Triaged. Jul 27th (2 years ago)
Unluckily I was sick last week and there was no time to transfer over potential communication.

Is this issue resolved now with the upcoming fix for 19.0.2?

dschuermann posted a comment. Jul 29th (2 years ago)
Currently on vacation. Can you point me to the commit?

bullzer posted a comment. Aug 12th (2 years ago)
Hi,

Sorry more vacations getting in the way it seems.
The commit is https://github.com/nextcloud/server/pull/21880

Cheers,
--Roeland

dschuermann posted a comment. Aug 12th (2 years ago)
Thanks. I just made the post public: https://hwsecurity.dev/2020/06/webauthn-pin-bypass/

dschuermann posted a comment. Aug 12th (2 years ago)
New URL because I updated the date:
https://hwsecurity.dev/2020/08/webauthn-pin-bypass/

bullzer posted a comment. Aug 19th (2 years ago)
Thanks. I forwarded the blog internally last week already.
Tomorrow RC1 of 19.0.2 comes out that has the fix. And thus it should be fixed next week on the final release.

Nextcloud has decided that this report is not eligible for a bounty. Aug 19th (2 years ago)

bullzer closed the report and changed the status to ○ Resolved. Aug 19th (2 years ago)
Thanks a lot for your report again. This has will be resolved in our next 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)

dschuermann posted a comment. Aug 20th (2 years ago)
Thanks, please mention us as:

Name / Pseudonym: Dominik Schürmann
Email address (optional): contact@cotech.de
Website (optional): https://www.cotech.de
Company (optional): COTECH

nickvergessen Nextcloud staff updated the severity from Low to Medium (4.3). Aug 24th (2 years ago)

Aug 24th (2 years ago)
nickvergessen Nextcloud staff changed the report title from **PIN Bypass in Passwordless WebAuthn on Nextcloud 19** to **PIN for passwordless WebAuthn is asked for but not verified**.

nickvergessen Nextcloud staff posted a comment. Aug 24th (2 years ago)
Requested CVE is CVE-2020-8236
Advisory will be published at https://nextcloud.com/security/advisory/?id=NC-SA-2020-037

Scheduled for 22nd of September

nickvergessen Nextcloud staff requested to disclose this report. Sep 28th (2 years ago)

This report has been disclosed. Oct 28th (2 years ago)