2

Improper confidentiality protection of server-side encryption keys

Share:

TIMELINE

yahe submitted a report to Nextcloud. Nov 21st (3 ye

This vulnerability is related to the Improper integrity protection of server-side encryption keys vulnerability but leverages a different attack vector. While the prev attack broke the confidentiality of encrypted files because the public keys are not integrity-protected, this new attack breaks the integrity of encrypted files beca the confidentiality of the public keys is not properly protected. As before, this attack also works with per-user key encryption.

Optional prerequisite: If you want to generate authenticated files that are AES-256-CTR encrypted, you have to know how many versions of a file there have beer Oftentimes it will just be `1` or you can denote the number of previous versions thanks to the default versioning plugin that stores old versions on disk as well. An external storage provider will have the possibility to know the version of a certain file by counting the write accesses to encrypted files. **But** you can also just use tl previously supported AES-256-CFB encryption which allows you to just skip the "signing" of the file.

How to do this:

- Generate a fresh file key (e.g. with `openssl rand -hex 32`)
- Generate a fresh envelope key (e.g. with `openssl rand -hex 16`)
- Encrypt the file key with the envelope key (e.g. with `encrypt-filekey.php` [1]) and replace the original `fileKey` file of the file you want to attack with the newly generated file
- Encrypt the envelope key with all public keys (they're stored as plain PEM-encoded keys on disk) that have currently access to the file (e.g. with `encrypt-envelopekey.php` [2]) and replace the corresponding `<username>.shareKey` files with the newly generated files
- Take the file that you want to modify and calculate its unencrypted file size (e.g. with `calculate-filesize.php` [3])
- Prepare a file with the same size and encrypt it for the newly generated file key (e.g. with `encrypt-file.php` [4]). If you use the AES-256-CTR encryption, then have to know the version number of the file or you can just use the AES-256-CFB encryption which doesn't require you to know the version number of the file (**optional** prerequisite).

The Nextcloud server-side encryption currently is not able to distinguish between a file that has been encrypted by the server itself and a file that has been encryp by a malicious attacker who has access to the Nextcloud data directory. This also holds true for setups where the administrator moved the whole data directory tc remote storage provider (through davfs2, s3fs, sshfs or similar) as this provider will then also be able to access the required key material.

[1] https://github.com/syseleven/nextcloud-tools/blob/master/encrypt-filekey.php
[2] https://github.com/syseleven/nextcloud-tools/blob/master/encrypt-envelopekey.php
[3] https://github.com/syseleven/nextcloud-tools/blob/master/calculate-filesize.php
[4] https://github.com/syseleven/nextcloud-tools/blob/master/encrypt-file.php

Impact

An attacker who has access to the encrypted files and the public keys of the users is able to replace encrypted files with properly encrypted (and **optionally** proper authenticated/"signed") files as long as the length of the new file contents matches the length of the old file contents.

1 attachment:
F640388: nextcloud_poc5.mp4

OT: posted a comment. Nov 21st (3 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 tc you to not disclose this issue to any other party.

ullzer posted a comment. Nov 25th (3 ye

Hi,

Thanks. I'll also take this into consideration when diving into the server side encryption code.
I'll get back to you.

Cheers,
--Roeland

nickvergessen Nextcloud staff changed the status to ○ Triaged. Dec 6th (3 ye

yahe posted a comment. Jan 21st (3 ye

Hi, I guess that now that Nextcloud 18 has been published there will be the time to look into the issues of the server-side encryption? My plan is to to submit a talk about the Nextcloud server-side encryption to the upcoming Gulaschprogrammiernacht (May 21st to May 24th). This should be enough time to fix the issues.

yahe posted a comment. May 27th (3 ye

Hello, this issue hasn't seen any update for 4 months. We approached the end of May without a fix. Do you still intend to work on this problem?

ullzer posted a comment. May 29th (3 ye

Cheers,
--Roeland

rullzer posted a comment. Aug 11th (2 ye

Hi,

Please see also https://github.com/nextcloud/server/pull/21529/files here
I think this also helps a lot in mitigating this attack vector.

Cheers,
--Roeland

yahe posted a comment. Aug 11th (2 ye

I think so, too.

rullzer posted a comment. Aug 24th (2 ye

Hi,

Ok this got merged into 20.
It is already in the beta1.

Cheers,
--Roeland

yahe posted a comment. Oct 5th (2 ye

Hi, I've seen that you have announced Nextcloud 20 that contains the fix for this issue. Will there be a security advisory for this issue?

nickvergessen Nextcloud staff closed the report and changed the status to ● Resolved. Oct 6th (2 ye

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

nickvergessen Nextcloud staff posted a comment. Oct 6th (2 ye

@yahe do you still not want bounties?

nickvergessen Nextcloud staff posted a comment. Oct 6th (2 ye

Disclosure planned for 1st November

https://nextcloud.com/security/advisory/?id=NC-SA-2020-040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8152

yahe posted a comment. Oct 6th (2 ye

As said, merch would be welcome. :)

yahe posted a comment. Oct 6th (2 ye

Concerning the crediting in the advisory:

Name: Kevin "Kenny" Niehage
E-Mail: kenny@syseleven.de
Website: https://www.syseleven.de/
Company: SysEleven GmbH

yahe posted a comment. Nov 5th (2 ye

Good morning. Do you already know when the CVE and NC-SA will be published?

nickvergessen Nextcloud staff posted a comment. Nov 5th (2 ye

Should be by now, I'm a bit overloaded currently. Will take care of it tomorrow (for all your issues)

yahe posted a comment. Nov 6th (2 ye

Looking forward to the publication of the CVEs and NC-SAs. :)

yahe requested to disclose this report. Nov 6th (2 ye

yahe posted a comment. Nov 9th (2 ye

Unfortunately, you don't seem to have had the necessary time on Friday to take care of this. Will you have time for it this week?

yahe posted a comment. Nov 13th (2 ye

@nickvergessen Good morning. Unfortunately, a **full week** has passed without the publication of the CVEs and NC-SAs. Will you find the time today?

nickvergessen Nextcloud staff posted a comment. Nov 13th (2 ye

The CVEs are published automatically when the linked issues are published, so let me do that.

nickvergessen Nextcloud staff agreed to disclose this report. Nov 13th (2 ye

SA published, CVE should autopublish when this is disclosed.

This report has been disclosed. Nov 13th (2 ye