8

Message Authentication Codes calculated by the Default Encryption Module allow an attacker to silently overwrite blocks in a file

Share:

TIMELINE

yahe submitted a report to Nextcloud. Jul 26th (3 years ago)

First: The default encryption module bundled with the Nextcloud Server creates SHA256-HMAC based message authentication codes for each individual 6072 byte-sized block of data. These are the steps to calculate the MAC:

- Take the user password and harden it with SHA256-PBKDF2 (denoted as `$passPhrase` in [1]).
- Concatenate `$passPhrase`, `$version` (which is the value `encrypted` from the `oc_filecache` table), `$position` (which is the zero-based index of the encrypted block within the file) and `"a"` and create a SHA512 hash of it (denoted as `$passPhrase` in [2]).
- Most MACs of file blocks are created under the salt `hash('sha512', $passPhrase.$version.$position."a", true)` with the exception of the last file block which uses the salt `hash('sha512', $passPhrase.$version.$position."end"."a", true)`,
- Finally create a SHA256-HMAC of the data under the salt `$passPhrase` (as seen in [3]).

Second: An encrypted file uses the same file key (stored in the corresponding `fileKey` file) and envelope keys (stored in the corresponding `shareKey` files) as its stored file versions.

Third: To prevent a file from being truncated the last block uses a different salt (containing `"end"`). To prevent file blocks from being moved within a file each message authentication key contains the `$position` of the block within the file. To prevent file blocks from being moved between different versions of the same file each message authentication key contains the `$version` of the file.

Fourth: However, the concatenation that is used to create message authentication key is ambiguous. It is e.g. not possible to differentiate between the block with `$position` 10 in `$version` 1 of a file (being `$passPhrase."1"."10"."a"`) and the block with `$position` 0 in `$version` 11 of a file (being `$passPhrase."11"."0"."a"`). This way the contents of a properly encrypted and signed file can be modified without breaking the signature check.

Fifth: The following steps describe a simple proof of concept:

Create a file consisting of 6072 * 10 "A" + 6072 "B" + 1 "1":

Code 84 Bytes Wrap lines Copy Download

```
php -r 'print(str_repeat("A", 6072*10).str_repeat("B", 6072)."1");' >./collision.txt
```

Upload the file to Nextcloud and visit the folder in which Nextcloud stored the encrypted and signed version of the file `./collision.txt`. Create a backup of the encrypted version 1:

Code 36 Bytes Wrap lines Copy Download

```
cp ./collision.txt ./collision.txt.1
```

Open the file in Nextcloud text editor and create 11 versions. The easiest way to do this is to scroll to the end of the file, add a character, press CTRL+S twice to make sure that the version has been created and proceed until the file has reached version 11. This can be checked in the database by issuing the following query:

Code 70 Bytes Wrap lines Copy Download

```
select encrypted from oc_filecache where path = 'files/collision.txt';
```

Download the file to have a sample of the currently valid version of the file. Then overwrite the file block with `$position` 0 of `./collision.txt` with the file block with `$position` 11 of `./collision.txt.1`.

Code 86 Bytes Wrap lines Copy Download

```
dd if=./collision.txt.1 of=./collision.txt bs=8192 conv=notrunc skip=11 seek=1 count=1
```

Download the file again. When comparing the first download of the file with the second download of the file you should see that the first block of the file has been modified without breaking the signature check.

1) apps/encryption/lib/Crypto/Crypt.php#L194
2) apps/encryption/lib/Crypto/Crypt.php#L505
3) apps/encryption/lib/Crypto/Crypt.php#L506

Impact

An attacker that has permanent access to the file storage like an administrator or external storage provider can learn how many versions of which files exist without needing access to the database by monitoring the created version files over time.

Such an attacker is able to modify the contents of files by overwriting certain file blocks with specific file blocks from earlier versions of the same files. This file modification is possible **without** having access to any encryption secrets like passwords or keys.

This attack works against master-key encrypted files as well as against user-key encrypted files.

1 attachment:
F539930: nextcloud_poc.mp4

OT: posted a comment. Jul 26th (3 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.

rullzer posted a comment. Aug 1st (3 years ago)

Cheers,
--Roeland

rullzer changed the status to Triaged. Aug 5th (3 years ago)

yahe posted a comment. Sep 3rd (3 years ago)

Hi, this topic hasn't been handled for a month now. Is there any update on this issue?

rullzer posted a comment. Sep 3rd (3 years ago)

Hi,

we have been very busy with the 17 release. So sorry for the lack of updates.

I managed to reproduce your issue.

Just to make sure I fully get the issue. This would allow an attacker to corrupt the files with previous encrypted data right? (I just want to make sure we are not missing anything).

I am in contact with the original author of that code to see if we can harden against this by using proper delimiters.

Cheers,
--Roeland

yahe posted a comment. Sep 4th (3 years ago)

Yes, that's exactly what this vulnerability could be used for.

yahe posted a comment. Oct 8th (3 years ago)

Hi, another month has gone by without any progress. Is there any update on this?

yahe posted a comment. Nov 8th (3 years ago)

And yet another month has gone by. Do you have any news on this?

yahe posted a comment. Jan 21st (3 years ago)

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 years ago)

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?

rullzer posted a comment. May 29th (3 years ago)

Hi,

Yes this is still on our list but right now we don't have a good way to solve it.

Cheers,
--Roeland

rullzer posted a comment. Aug 11th (2 years ago)

Hi,

So we have been looking into this as well.
We think we have a solution but it might not solve all the cases (but at least a lot). I'll send you a PR soon. It would be great if you could have a look as well.

Cheers,
--Roeland

rullzer posted a comment. Aug 11th (2 years ago)

Hi,

So we could not identify a solution for existig files. But for new files/versions. Please see:
https://github.com/nextcloud/server/pull/22196

basically we just add a '_' in between the different parts of the passphrase. That should make sure this does not happen anymore.

Some side notes

1 This requires the file to be modified to write the new signature
2 Because of the fallback to the old method. Attackers that were in the process of doing this attak can continue it for a little while longer.

However I still think for now it is the best to do. As iterating over all files is not doable with huge installations (and millions of files).

For future work I have the idea to check if there is 1 new signature in the file to require all new signatures. That would make it even harder to abuse this. However that required a lot deeper changes for which it is way to hot right now.

Cheers,
--Roeland

yahe posted a comment. Aug 11th (2 years ago)

I think this is a simple but effective solution.

ullzer posted a comment. Aug 12th (2 years ago)

Hi,

Ah good point. Of course they still lose data. And an attacker could already have the data they need. But it is still a good idea.

Let me get this reviewed and merged (and backported since it is just 2 lines of code).

Cheers,
--Roeland

ullzer posted a comment. Aug 12th (2 years ago)

Hi,

Small update. This just got merged into master. And the backports to all the maintenance releases are pending.

Cheers,
--Roeland

extcloud rewarded yahe with a **$250** bounty. Aug 24th (2 years ago)

Congratulations! We have determined this to be eligible for a reward of $250.

Thanks a lot for making the internet a safer place and keep hacking. Please keep in mind that we didn't release the fix yet, so please do not share this information with any third-parties.

ullzer closed the report and changed the status to ○ **Resolved**. Aug 24th (2 years ago)

Thanks a lot for your report again. This will be 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)

yahe posted a comment. Aug 24th (2 years ago)

Hi, thanks for assigning a bounty to this. Would it be possible to get a couple of Nextcloud merch t-shirts instead of the money so that I can share them with my colleagues?

Concerning the information:

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

ullzer posted a comment. Aug 24th (2 years ago)

Hi,

I don't think we can unassign a bounty. But for the others we could of course. I'm not sure if we currently have a lot of t-shirts left (normally they get ordered now but our conference goes online this year). But let me check for some swag. Would you rather have swag than money?

Cheers,
--Roeland

yahe posted a comment. Aug 24th (2 years ago)

Yes, swag would be appreciated. :)

ullzer posted a comment. Aug 24th (2 years ago)

Ok. I've asked if we have any left. But otherwise I'll make sure you are on the list for a few once they are back in stock. Together with a bunch of stickers of course :)

yahe posted a comment. Oct 5th (2 years ago)

Hi, I've seen that you have announced Nextcloud 20 and have also backported this fix to Nextcloud 17, 18 and 19. Will there be a security advisory for this issue?

nickvergessen Nextcloud staff posted a comment. Oct 6th (2 years ago)

Yeah, sorry with the conf and the release we have quite a todo backlog. Advisories will come (but we publish them 4 weeks after the release only anyway).

Oct 6th (2 years ago)

nickvergessen Nextcloud staff

changed the report title from **Message Authentication Codes calculated by the Default Encryption Module allow an attacker to silently overwrite blocks in a file** to **Passphrase codes calculated by the Default Encryption Module can overwrite each others**.

Oct 6th (2 years ago)

nickvergessen Nextcloud staff

changed the report title from **Passphrase codes calculated by the Default Encryption Module can overwrite each others** to **Message Authentication Codes calculated by the Default Encryption Module allow an attacker to silently overwrite blocks in a file**.

nickvergessen Nextcloud staff requested to disclose this report. Oct 6th (2 years ago)

nickvergessen Nextcloud staff posted a comment. Oct 6th (2 years ago)

This report has been disclosed. Nov 5th (2 years ago)

yahe posted a comment. Nov 5th (2 years ago)

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

nickvergessen Nextcloud staff posted a comment. Nov 13th (2 years ago)

SA and CVE published