Jump to bottom New issue

Oc_credentials security? #17439

⊙ Closed tanguy-opendsi opened this issue on Oct 7, 2019 · 13 comments

0. Needs triage enhancement Labels

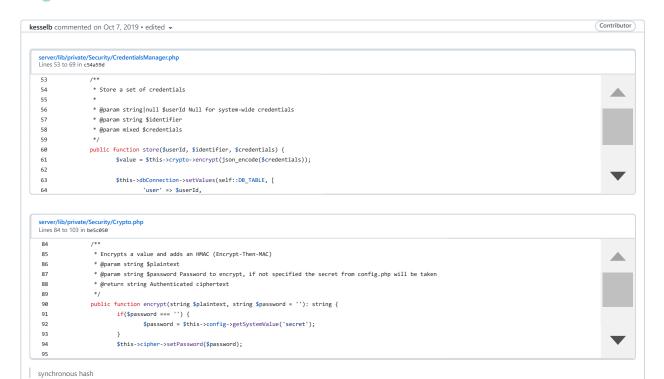
tanguy-opendsi commented on Oct 7, 2019

Can i get informations about the algorithm used to hash password inside oc_credentials.

I think this is synchronous hash because nextcloud need it with external storage but i'm not sure ?

Best regards

tanguy-opendsi added 0. Needs triage enhancement labels on Oct 7, 2019



kesselb closed this as completed on Oct 7, 2019

Sure. Everything is open. Please use https://help.nextcloud.com for questions.

Schmuuu commented on Oct 7, 2019

Can i get informations about the algorith

Hi @kesselb

I would say yes.

Just to let you know, I told him to better ask the developers regarding these questions. We in the Forum don't have much of the insights. Especially when it comes to questions why certain hash functions have been chosen, the broader community is missing the information I think.

kesselb commented on Oct 7, 2019

Contributor

told him to better ask the developers regarding these questions

Seems valid. Do you think the answer is sufficient? We can still ping some of the paid engineers. But the question is not specific.

Schmuuu commented on Oct 8, 2019

Thanks :)

Well, I'm not sure; @tanguy-opendsi does this answer your question?

The comment seems to be descriptive: "Encrypts a value and adds an HMAC (Encrypt-Then-MAC)"

And the DB table oc_credentials seems to save a value consisting of

ciphertext|iv|hmac

where "iv" seems to be a random number based on the length of an string. I don't understand what iv could mean or what ivLength is about. But maybe you understand that. Please let us know what your questions was aiming at and where further clarification is required.

tanguy-opendsi commented on Oct 8, 2019

Author

kesselb commented on Oct 8, 2019

Contributor

cc @nextcloud/security 🏓

LukasReschke commented on Oct 8, 2019

Member

IV = Initialization Vector, which is required as this is using AES in CBC mode.

https://en.wikipedia.org/wiki/Initialization_vector has some more details.

tanguy-opendsi commented on Oct 8, 2019

Author

@LukasReschke that mean HMAC use AES?

LukasReschke commented on Oct 8, 2019

Member

The HMAC is there to provide integrity. AES CBC alone doesn't provide that.

The answer at https://security.stackexchange.com/questions/63132/when-to-use-hmac-alongside-aes is describing this quite well.



LukasReschke commented on Oct 8, 2019

Member

I guess it would be good if you could rephrase your original question so that we can give a better answer :-)

What are your concerns? What do you want to protect against?

tanguy-opendsi commented on Oct 8, 2019

Author

@LukasReschke

Ok:)

My question is :

How work the mechanism when you use external storage?

Nextcloud have to store and decrypt the password to use external storage properly ?

If yes, what is the strength of your code (Using salt, what algorithm ect..)

Can you describe the mechanism ?

olivluca commented on May 19, 2020

Isn't it futile to encrypt the password, considered that if an attacker compromises the system he can easily obtain the secret?

I'd much prefer for the password not to be stored if there is no need for them, yet they are even if I have no external storage configured with stored credentials.

kesselb commented on May 19, 2020

Contributor

@olivluca #21037

Assignees

No one assigned

Labels

0. Needs triage enhancement

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants





