End-to-end encryption device setup did not verify public key

Moderate **LukasReschke** published **GHSA-f5fr-5gcv-6cc5** on Aug 18, 2021

Package	
Desktop Client (Nextcloud)	
Affected versions	Patched versions
< 3.3.0	3.3.0

Description

Impact

Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint as described in the RFC:

> In case a certificate exists already for the user the client has to download the existing private key. This is done the following way:
>
> 1. Client downloads private key from the /ocs/v2.php/apps/end_to_end_encryption/api/v1/private-key endpoint.
> 2. Client asks the user for the mnemonic and decrypts the private key using AES/GCM/NoPadding as cipher (256 bit key size) and PBKDF2WithHmacSHA1 as key derivation.
> 3. Client checks if private key belongs to previously downloaded public certificate.
> 4. Client checks if their certificate was signed by the server (checking the servers public key from /ocs/v2.php/apps/end_to_end_encryption/api/v1/server-key)
> 5. Client stores the private key in the keychain of the device.
> 6. The mnemonic is stored in the keychain of the device (ideally with spaces so it can be shown more readable).

The Nextcloud Desktop client skipped the third step: "Client checks if private key belongs to previously downloaded public certificate." - If the Nextcloud instance served a malicious public key, the data would be encrypted for this key and thus could be accessible to a malicious actor.

Patches

It is recommended that the Nextcloud Desktop client is upgraded to 3.3.0.

Workarounds

None.

References

- HackerOne
- Pull Request

For more information

If you have any questions or comments about this advisory:

- Create a post in nextcloud/security-advisories
- Customers: Open a support ticket at support.nextcloud.com

Severity

Moderate

CVE ID

CVE-2021-32728

Weaknesses

CWE-295

Credits

robottod