127 Missing ownership check on remote wipe endpoint

Share:

TIMELINE

hitman_47 submitted a report to Nextcloud. Mar 15th (3 years ago)

On settings/user/security

You can mark a device for wipe out that does not belong to you.

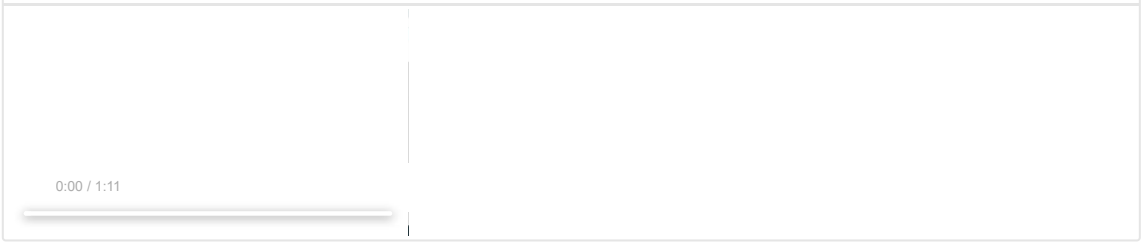
Steps:

1. Create 2 accounts one for the hacker and one for the victim
2. On both accounts add devices with different names
3. On the hacker account, while intercepting with burpsuite, select the option to wipe out a device
4. Forward with burpsuite and in the url that looks like settings/personal/authtokens/wipe/{data-id}, change the data-id to the id of the device of the victim
5. Stop intercepting or forward again and the device of the victim will be marked for wipe out.

Here is a video demo

Video F748890: IDORNextCloud.mp4 6.53 MiB

Zoom in Zoom out Copy Download



Impact

Attacker can wipe out the device of another user by using the device ID

1 attachment:
F748890: IDORNextCloud.mp4

OT: posted a comment. Mar 15th (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.

hitman_47 updated the severity to High. Mar 15th (3 years ago)

nickvergessen Nextcloud staff changed the status to o Triaged. Mar 16th (3 years ago)

Confirmed, thanks for the report

nickvergessen Nextcloud staff updated the severity from High to High (7.7). Mar 16th (3 years ago)

nickvergessen Nextcloud staff posted a comment. Mar 16th (3 years ago)

We are currently working on the patch and the following one seems to solve it:

Code 1.47 KiB Wrap lines Copy Download

```
diff --git a/apps/settings/lib/Controller/AuthSettingsController.php b/apps/settings/lib/Controller/AuthSettingsController.php
index 7248127fd6..ccd1d370a1 100644
--- a/apps/settings/lib/Controller/AuthSettingsController.php
+++ b/apps/settings/lib/Controller/AuthSettingsController.php
@@ -289,7 +289,7 @@ private function findTokenByIdAndUser(int $id): IToken {
        * @throws \OC\Authentication\Exceptions\ExpiredTokenException
        */
       public function wipe(int $id): JSONResponse {
-        if (!$this->remoteWipe->markTokenForWipe($id)) {
+        if (!$this->remoteWipe->markTokenForWipe($id, $this->uid)) {
             return new JSONResponse([], Http::STATUS_BAD_REQUEST);
         }

diff --git a/lib/private/Authentication/Token/RemoteWipe.php b/lib/private/Authentication/Token/RemoteWipe.php
index 2285ccd2cd..b3555203c6 100644
--- a/lib/private/Authentication/Token/RemoteWipe.php
+++ b/lib/private/Authentication/Token/RemoteWipe.php
@@ -58,17 +58,17 @@ public function __construct(IProvider $tokenProvider,

```

```
23 +     * @param string $userId
24       * @return bool
25       *
26       * @throws InvalidTokenException
27       * @throws WipeTokenException
28       * @throws ExpiredTokenException
29       */
30 -    public function markTokenForWipe(int $id): bool {
31 +    public function markTokenForWipe(int $id, string $userId): bool {
32           $token = $this->tokenProvider->getTokenById($id);
33
34 -         if (!($token instanceof IWipeableToken)) {
35 +         if (!$token instanceof IWipeableToken || $token->getUID() !== $userId) {
36               return false;
37           }
38
```

In case you want to confirm it

hitman_47 posted a comment. Mar 16th (3 years ago)

Great!, thanks for the quick follow up

hitman_47 posted a comment. Mar 17th (3 years ago)

So I tested again and I can confirm this vulnerability has been patched. Great job on fixing it so quickly.

nickvergessen Nextcloud staff closed the report and changed the status to **Resolved**. Mar 20th (3 years ago)

Thanks a lot for your report again. This has been 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)

Nextcloud rewarded hitman_47 with a **$500** bounty. Mar 20th (3 years ago)

hitman_47 posted a comment. Mar 20th (3 years ago)

Thank you so much for the Bounty :). I can be credited as Tommy Suriel.

hitman_47 requested to disclose this report. Mar 20th (3 years ago)

Can you disclose this report?

nickvergessen Nextcloud staff posted a comment. Mar 20th (3 years ago)

We will with the normal 4 weeks delay between release (monday) and disclosure (20th of april).
Together with an advisory on https://nextcloud.com/security/advisories and a CVE.

CVE will be requested soon, the advisory will be published under the id 2020-018: https://nextcloud.com/security/advisory/?id=NC-SA-2020-018

hitman_47 posted a comment. Updated Mar 20th (3 years ago)

Perfect, I look forward to those releases. Thank you again.

This report has been disclosed. Apr 19th (3 years ago)

nickvergessen Nextcloud staff changed the scope from **Desktop Client** to **nextcloud/server**. Apr 22nd (3 years ago)

Apr 22nd (3 years ago)

nickvergessen Nextcloud staff changed the report title from **IDOR allows me to mark devices of another user for remote wipe out** to **Missing ownership check on remote wipe endpoint**.