

10

No rate limiting on sinup page

Share:     

TIMELINE



xam24 submitted a report to [Nextcloud](#).

Jul 13th (2 ye

Hi Team,

Summary:

As a best practice a login page should have a rate limiting.

Below is the captured request of respective login page of nextcloud.com

POST /index.php/apps/preferred_providers/password/submit/D4oCzV7LrgyTtULRXsOp2 HTTP/1.1

Host: efss.qcloud.my

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 65

Origin: null

Connection: close

Cookie: ocn6e46ay0uf=g5gaufmdvaa2ab480r3m3e2fp;

oc_sessionPassphrase=rXsGoXrFnFnMxJG7wqHo25XUJ75w4gCINgeLpQ6nUy8GJQel2%2F14gFzllhagLg7o8uulcNuNIWKdhzxUtdyDoPaPPqsSqHk6xbJYMKuVvM%2BJ%2Bz8rB6%2B9j25LcYT; Host-nc_sameSiteCookieIax=true; Host-nc_sameSiteCookieIstrict=true

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

ocsapirequest=&email= <targer username> &password= <target password>

Steps to reproduce :

1. Tamper login page and send the request to Burp Intruder.
2. Configure the payloads
3. Start the Burp Intruder

POC:

in the attached image.

As you can see i have sent more than 85 requests ,

Therefore all the requests are being exexuted with response code 200

Impact

Impact:

An attacker can freely bruteforce any username and can takeover any account.

1 attachment:

[F905420: nextcloud1.png](#)



OT: posted a comment.

Jul 13th (2 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 to you to not disclose this issue to any other party.



xam24 posted a comment.

Jul 13th (2 ye

Correction*

Steps to reproduce:

1. Tamper the signup page and send request to Burp Intruder



xam24 posted a comment.

Jul 15th (2 ye

Any update ?



nickvergessen (Nextcloud staff) changed the status to Triaged.

Jul 27th (2 ye

I will poke the relevant persons again, but currently summer season is kicking in and the remaining persons need to prioritize harder and this is currently not at the of the list.



nickvergessen (Nextcloud staff) posted a comment.















Jul 29th (2 ye

Pull request is at https://github.com/nextcloud/preferred_providers/pull/18



xam24 posted a comment.

Jul 29th (2 ye

<p> Nextcloud staff posted a comment.</p> <p>I just posted above that we fixed the issue.</p> <p>We have to do a release and then the providers can deploy this.</p>	Jul 29th (2 ye
<p> posted a comment.</p> <p>What about bounty , is there any update about that?</p>	Jul 29th (2 ye
<p> posted a comment.</p> <p>Any update?</p>	Jul 30th (2 ye
<p> posted a comment.</p> <p>Any update about the program @nickvergessen @Nextcloud. ??</p>	Aug 1st (2 ye
<p> Nextcloud staff closed the report and changed the status to Resolved.</p> <p>1.8.0 of the preferred providers app has been published this morning. It's therefor now up to the providers to update their installations</p>	Aug 3rd (2 ye
<p> Nextcloud rewarded xam24 with swag.</p> <p>The preferred providers app is not eligible for bounties.</p>	Aug 3rd (2 ye
<p>○ Nextcloud has decided that this report is not eligible for a bounty.</p>	Aug 3rd (2 ye
<p> Nextcloud staff posted a comment.</p> <p>Thanks a lot for your report again. This has been resolved in the latest maintenance release and we're working on the advisories at the moment.</p> <p>Please let us know how you'd like to be credited in our official advisory. We require the following information:</p> <ul style="list-style-type: none"> • Name / Pseudonym • Email address (optional) • Website (optional) • Company (optional) 	Aug 3rd (2 ye
<p> posted a comment.</p> <p>Nice working with you 😊</p> <p>Here are my details .</p> <p>Name: Faeeq jalali</p> <p>Email: faeeqjalali24@gmail.com</p>	Aug 3rd (2 ye
<p> posted a comment.</p> <p>Can I know in how many day the swag will be delivered?</p>	Aug 3rd (2 ye
<p> Nextcloud staff posted a comment.</p> <p>Can I know in how many day the swag will be delivered?</p> <p>As far as I know we are currently out of stock and our conference in september was cancelled due to covid19, so there was no reorder so far. might take until the next conf beginning of next year :/</p>	Aug 3rd (2 ye
<p> posted a comment.</p> <p>Ok thank you .</p>	Aug 3rd (2 ye
<p>○ nickvergessen Nextcloud staff updated the severity from High to <u>Low (3,5)</u>.</p>	Aug 3rd (2 ye
<p>○ nickvergessen Nextcloud staff changed the scope from https://customerupdates.nextcloud.com to https://nextcloud.com.</p>	Aug 3rd (2 ye
<p> posted a comment.</p> <p>Hey Nextcloud</p> <p>Its been weeks since the report is resolved.</p> <p>And I have no information about the swag.</p> <p>Please update me about the swag</p> <p>When am I going to get it?</p>	Aug 17th (2 ye
<p> Nextcloud staff posted a comment.</p> <p>Aparently we are currently out of tshirts and since our conference this year was canceled due to corona, no new tshirts were ordered. So it might take until next year conference before we have some again.</p>	Aug 18th (2 ye
<p>○ nickvergessen Nextcloud staff requested to disclose this report.</p>	Sep 28th (2 ye
<p>○ xam24 agreed to disclose this report.</p>	Sep 28th (2 ye
<p>○ This report has been disclosed.</p>	Sep 28th (2 ye
<p> posted a comment.</p>	Nov 28th (2 ye



See previous message



xam24 posted a comment.
Any update on swag?

Jan 28th (2 ye

