No rate limiting on sinup page

Share: f in Y

TIMELINE



Jul 13th (2 ye

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

Below is the captured request of respective login page of next cloud.com

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

Host: efss.gloud.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=g5gaufmdvaa2ab480rl3m3e2fp;

 $oc_session Passphrase = rXsGoXrFnFNmXjG7wqHo25XUJ75w4gClNgeLpQ6nUy8GJQel2%2F14gFzllhagLg7o8uulcNuNiWKdhzxUtdyDoPaPPsqsSqHk6xbJYMK$ $uVvM\%2BJ\%2Bz8rB6\%2B9j25LcYT; \textbf{Host-nc_sameSiteCookielax=true}; Host-nc_sameSiteCookiestrict=true \\$

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

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

1 attachment:

F905420: nextcloud1.png



Jul 13th (2 ye

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 the factor of the properties of the pryou to not disclose this issue to any other party.

m24 posted a comment. Correction*

Jul 13th (2 ye

Steps to reproduce:

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

m24 posted a comment. Any update?

Jul 15th (2 ye

ickvergessen (Nextcloud staff) changed the status to • Triaged.

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.

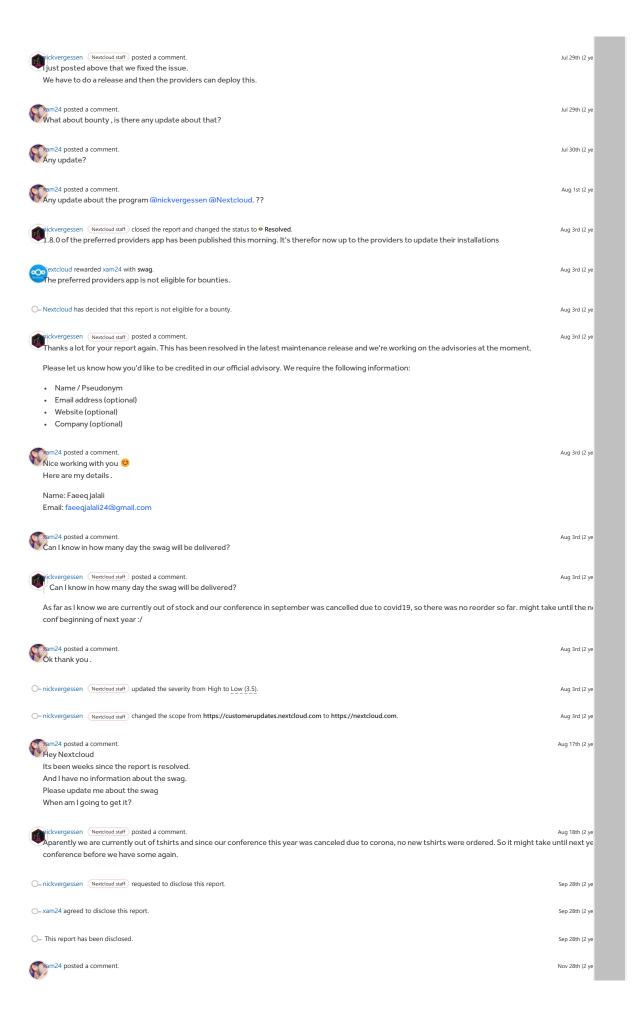
ckvergessen (Nextcloud staff) posted a comment.

Jul 29th (2 ye

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



Jul 29th (2 ye





Jan 28th (2 ye