More Create Riog Sign In

code16

Strona główna Mini arts Notes Magazine Found bugs CTFs Contact

CZWARTEK, 20 SIERPNIA 2020

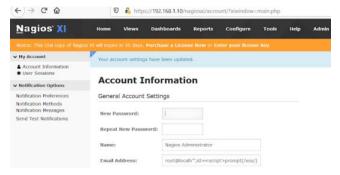
Postauth RCE in Nagios 5.7.2

Last time when I was checking NagiosXI is described here[1, 2, 3] so you could already get some 'basic introduction' to the topic. Below you will find new more details - this time for (again) 'latest' version (5.7.2). Here we go...

This time we will start here



As usual I tried to identify some webapps bugs like XSS (to 'start somehere';)). So I started here:



I found that 'Email Address' is vulnerable to XSS, see below:



In the meantime I was looking for the reason in the source. This is one of the findings:



Next I watched NagiosXI weblog console, check this out (looks pretty familiar to few last cases described here):



Well...;> I started to dig a bit with this field...

O MNIE



code16
Cody Sixteen
Wyświetl mój pełny

ARCHIWUM BLOGA

- **▶** 2022 (16)
- ► 2021 (37) ▼ 2020 (62)
- 2020 (62)► 12 (1)
- ► 11 (2)
- **▶ 10** (1)
- **▶** 09 (2)
- ▼ 08 (5)

Scanning Docker Images

Creating your first CTF VM

Basic Pentest Lab with Docker

Postauth RCE in Nagios

Scheduling Checkpoint Gaia

- **▶** 07 (5)
- **▶** 06 (7)
- **▶** 05 (5)
- ► 04 (11) ► 03 (10)
- **▶** 02 (6)
- **▶** 01 (7)
- **▶** 2019 (97)
- **▶** 2018 (67)
- **▶** 2017 (58)
- **2016** (63)

ETYKIETY

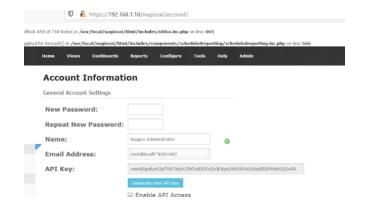
web

writeup

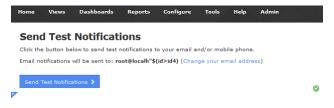
net
android
binary

crackme

ctf
debug
docker
drones
enili
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc
pwn



After I updated my account-email-settings I decided to send test notifications:



Few more attempts below:



...and 'few more' (hours of) checking source and logs:

```
| Content and form of the content of
```

And that's how I found this file:

Going down?

```
// Subait the event
$event_meta = arcsyOr => $val) (
$event_meta [svar] = $val;
}

// Email notifications
if (isset($mms! [contactemail']) && isset($mms['message']) && isset($mms['subject'])) {

if ($debug == true) {
    echo_("An email notification will be sent"),"...\n\n";
}

// Use this for debug output in PHPmailer log
$debugsag = "";

// Set where email is coming from for PHPmailer log
$send_mail_neferer = "scripts/contact_notification_handler.php > Notification Handler Script";

**The contact is a subject to the contact is
```

Now, let's parse_argv():

I was wondering if I'm able to even try to run "the same" command using directly (only) bash (from target server):

```
Two-tiles allow to-classes are the continued of the conti
```

I was. So the reason was something inside the webapp - not the payload itself... Checking:

```
Send Test Notifications

Send Test Notificatio
```

Here (from bash-perspective) everything looks fine. So I was looking more and more source files, github links, and google resources. After preparing a proper (but-still-bash) payload I decided to test it again using 'Send Test Notifications':

```
Send Test Notifications

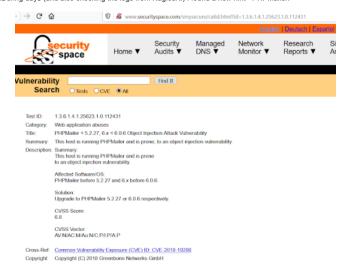
### Annual Control of the Control of the
```

No luck (screen from VMPlayer is the response for bash request started from runme.sh script).

I tried to ask *ps*|aux for some hint(s):

After 4 days...;] I even decided to try to use some strace-magic:

Still nothing. During day5 (and also checking the logs from NagiosXI) I found a new hint - PHPMailer:



Ok. So: in my opinion I wasn't able to escape from new version of PHPMailer available in NagiosXI. That was the reason (but feel free to correct me (and my payload;)) if I'm wrong).

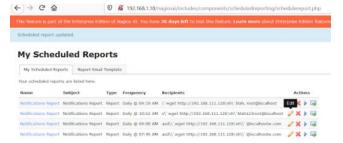
Few more pages to read I found for example here:

```
 \begin{tabular}{ll} \hline \textbf{0} & \textbf{https://github.com/PHPMailer/PHPMailer/blob/master/src/PHPMailer.php} \\ \hline \end{tabular} 
public function addReplyTo($address, $name = '')
    return $this->addOrEnqueueAnAddress('Reply-To', $address, $name);
^{\ast} Add an address to one of the recipient arrays or to the ReplyTo array. Because PHPMailer
* can't validate addresses with an IDN without knowing the PHPMailer::$CharSet (that can stil
 * be modified after calling this function), addition of such addresses is delayed until send(
\ensuremath{^{*}} Addresses that have been added already return false, but do not throw exceptions.
 * @param string $kind One of 'to', 'cc', 'bcc', or 'ReplyTo'
* @param string $address The email address to send, resp. to reply to
* @param string $name
 * @throws Exception
 * @return bool true on success, false if address already used or invalid in some way
protected function addOrEnqueueAnAddress($kind, $address, $name)
    $address = trim($address);
    $name = trim(preg_replace('/[\r\n]+/', '', $name)); //Strip breaks and trim
    $pos = strrpos($address, '@');
   if (false === $pos) {
        // At-sign is missing.
        $error_message = sprintf(
           '%s (%s): %s',
           $this->lang('invalid_address'),
           $kind,
           Saddress
```

Sample logs:

```
Notes that state of the provide at least one recipies and indirect. (without-require the includes ACMANIA CONTROL (ACMANIA CA
```

BTW: you can also (re)send your 'emails' (payloads) using 'My Scheduled Reports', check it out:



Few more example logs:

```
| Table | State | Stat
```

At this stage (day6;]) I decided to "leave it like this" here and go to the next (possible) bug (I'll found). So that's how I landed in one of the available Configuration Wizards:



I decided to give it a try (and prepare similar payload):



As you can see (last line on the screen above) there is an **echo-output**; **D** of the command we tried to use. ;] Great, let's try one more time:



This time we should be here:



Ok, again:

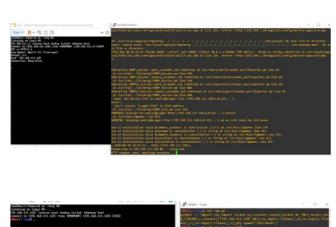


[; I think we're already there... ;] Checking:



(Yep, I saw fopen() so I tried to read some passwd;))

Now:



Bingo! ;]



Using few old tricks (like payload+base64+|sh) we should be somewhere here:



Waiting:



I think we'll stop here.

Special thanks goes to my Patreon: Daniel.

Thanks! You are awesome! ;)

See you next time!

Cheers

Posted by code16 at 09:29

Labels: debug, infrastructure, notes, pentest, pwn, web, writeup

Brak komentarzy:

Prześlij komentarz





Nowszy post Strona główna Starszy post

Subskrybuj: Komentarze do posta (Atom)

Motyw Okno obrazu. Obsługiwane przez usługę Blogger.