

Postauth RCE in Nagios 5.7.2

This time we will start **here**:



[Wyświetl mój pełny profil](#)

► **2022** (16)

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

Creating your first CTF VM

Postauth RCE in Nagios 5.7.2

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)

- [.net](#)
- [android](#)
- [binary](#)
- [crackme](#)
- [ctf](#)
- [debug](#)
- [docker](#)
- [drones](#)
- [enlil](#)
- [FortiGate](#)
- [fuzz](#)
- [infrastructure](#)
- [malware](#)
- [notes](#)
- [pentest](#)
- [poc](#)
- [pwn](#)
- [RE](#)
- [web](#)
- [writeup](#)

← → ↻ 🏠 https://192.168.1.10/nagiosxi/account/?xwindow=main.php

Nagios XI Home Views Dashboards Reports Configure Tools Help Admin

Notice: This trial copy of Nagios XI will expire in 30 days. Purchase a License Now or Enter your license key.

▼ My Account

- Account Information
- User Sessions

▼ Notification Options

- Notification Preferences
- Notification Methods
- Notification Messages
- Send Test Notifications

Your account settings have been updated.

Account Information


General Account Settings

New Password:

Repeat New Password:

Name:

Email Address:



The screenshot shows the Nagios XI web interface. At the top, there's a navigation bar with links: Home, Views, Dashboards, Reports, Configure, Tools, Help, Admin. Below this is a yellow banner with a notice: "Notice: This trial copy of Nagios XI will expire in 30 days. Purchase a License Now or Enter your license key." The main content area is titled "Test Email Settings". It contains a red box with the text: "A test email was sent to root@localhost.pld.pl". Below this is a text input field containing "test@". At the bottom right, there are two buttons: "OK" and "Cancel". On the left side, there's a sidebar with a tree view showing the navigation structure: Systems Information (System Status, Monitoring Engine Status, Audit Log, Check For Updates), Users (Manage Users, LDAP/AD Integration, Notification Management, User Sessions), and Systems Config (System Settings, License Information, Remote Configuration).

```
>>>root@kali:~/bin# cat /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/activerecord-6.0.3.2/lib/active_record/connection_adapters/abstract_adapter.rb:189: warning: method redefined; previous definition was here
```

[illegible]

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

https://192.168.1.10/nagiosxi/account/

afford 450 of 758 bytes in /usr/local/nagiosxi/html/includes/util.inc.php on line 465
plied for foreach) in /usr/local/nagiosxi/html/includes/components/scheduledreporting/scheduledreporting.inc.php on line 566

HomeViewsDashboardsReportsConfigureToolsHelpAdmin

Account Information

General Account Settings

New Password:

Repeat New Password:

Name:

Nagios Administrator

Email Address:

root@localhost\$(id-id4)

API Key:

emeH0gufueY2pT9d7WjvUZYn5aDD5eQeIEdgqLNV35k5eQyap1t00MebGQ3eGA

Generate new API key

Enable API Access

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

HomeViewsDashboardsReportsConfigureToolsHelpAdmin

Send Test Notifications

Click the button below to send test notifications to your email and/or mobile phone.
Email notifications will be sent to: **root@localhost\$(id-id4)** ([Change your email address](#))

Send Test Notifications

Few more attempts below:

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

And that's how I found this file:

Going down?

is the

Sample logs:

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

Few more example logs:

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

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

192.168.1.10/nagiosxi/config/monitoringwizard.php

Configuration Wizard: Network Switch / Router - Step 2

Switch Details

Switch/Router Address: 123.123.123.123
 Host Name: 23.123.123.123

Services

Specify which services you'd like to monitor for the switch or router.

☒ Ping
 Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

No ports were detected on the switch. Possible reasons for this include:

- The switch is currently down
- The switch does not exist at the address you specified
- SNMP support on the switch is disabled

Troubleshooting Tip:
 If you keep experiencing problems with the switch wizard scan, login to the Nagios XI server as the root user and execute the following command:

```
/usr/bin/cfengine --show-up-down --no-verbose --zero-speed "100000000" "public@123.123.123.123" "idb/123.123.123.123:123.123.123.123"
```

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:

192.168.1.10/nagiosxi/config/monitoringwizard.php?update=1&nextstep=2&nsp=43

Configuration Wizard: Network Switch / Router - Step 1

Router/Switch Information

IP Address: 123.123.123.123
 The IP address of the network device you'd like to monitor

Port: 161
 The port of the network device

This time we should be here:

192.168.1.10/nagiosxi/config/monitoringwizard.php

Configuration Wizard: Network Switch / Router - Step 2

Switch Details

Switch/Router Address: 123.123.123.123
 Host Name: 23.123.123.123

Services

Specify which services you'd like to monitor for the switch or router.

☒ Ping
 Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

No ports were detected on the switch. Possible reasons for this include:

- The switch is currently down
- The switch does not exist at the address you specified
- SNMP support on the switch is disabled

Troubleshooting Tip:
 If you keep experiencing problems with the switch wizard scan, login to the Nagios XI server as the root user and execute the following command:

```
/usr/bin/cfengine --show-up-down --no-verbose --zero-speed "100000000" "public@123.123.123.123" "idb/123.123.123.123:123.123.123.123"
```

Ok, again:

192.168.1.10/nagiosxi/config/monitoringwizard.php

Configuration Wizard: Network Switch / Router - Step 1

Router/Switch Information

IP Address: 123.123.123.123
 The IP address of the network device you'd like to monitor

Port: 161
 The port of the network device

SNMPv1 ☒ SNMPv2c ☒ SNMPv3

SNMP Community: public
 The SNMP community string required used to query the network device

Monitoring Options

Monitor Thing: Port's Number
 Select the port naming scheme that should be used.

Scan Interfaces ☒ Scan the switch or router to auto-detect interfaces that can be monitored for links.

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

192.168.1.10/nagiosxi/config/monitoringwizard.php

Configuration Wizard: Network Switch / Router - Step 2

Switch Details

Switch/Router Address: 123.123.123.123
 Host Name: 23.123.123.123

Services

Specify which services you'd like to monitor for the switch or router.

☒ Ping
 Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

No ports were detected on the switch. Possible reasons for this include:

- The switch is currently down
- The switch does not exist at the address you specified
- SNMP support on the switch is disabled

Troubleshooting Tip:
 If you keep experiencing problems with the switch wizard scan, login to the Nagios XI server as the root user and execute the following command:

```
/usr/bin/cfengine --show-up-down --no-verbose --zero-speed "100000000" "public@123.123.123.123" "idb/123.123.123.123:123.123.123.123"
```

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

Now:

Subskrybuj: [Komentarze do posta \(Atom\)](#)

Motyw Okno obrazu. Obsługiwane przez usługę Blogger.