

Nagios 5.6.11 XSS'd

The screenshot shows the Nagios website with the URL https://www.nagios.org/downloads/nagios-xi/vmware/vm7/product. The Nagios logo and tagline "The industry standard in IT Infrastructure Monitoring" are visible. A download dialog box is open, titled "Otwieranie nagiosxi-5.6.11-64.ova". It shows the file name "nagiosxi-5.6.11-64.ova" with a file icon, the format "Open Virtualization Format Archive (1,8 GB)", and the address "https://assets.nagios.com". Under the section "Po ukończeniu pobierania:", there are three options: "Otwórz za pomocą VirtualBox Manager (domyślny)", "Zapisz plik" (which is selected with a radio button), and "Pamiętaj tę decyzję dla wszystkich plików tego typu". At the bottom right are "OK" and "Anuluj" buttons.

Below you'll find few XSS bugs found for latest Nagios XI (5.6.11). All of them are available for admin user logged-in (so, those are postauth xss bugs). For example:

[illegible][illegible]

LDAP / Active Directory Import Users

Warning: ldap_() unable to bind to server: (LDAP error: LDAP server is down) The LDAP server host (hostname/ip address) and port (number) must be specified. Check the configuration file: /etc/ldap/ldap.conf

[Click here to automatically create an account for this LDAP user selected](#)

Only users using LDAP / Active Directory authentication or privileged accounts will be able to import users.

asid

password

OK Cancel

```
700 }
701
702 // Hint on the user
703 user = false;
704 this->labelled = false; this->labelConnection = true; user = this->getConnection(), user = true;
705 if (this->labelled)
706     user = true;
707
708 // Once we've checked their details, click back into admin mode if we have it
```

[illegible]

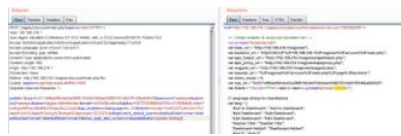
Cody Sixteen

Wyświetl mój pełny profil

► **2022** (16)

- ▶ 02 (6)
- ▶ 01 (7)
- ▶ 2019 (97)
- ▶ 2018 (67)
- ▶ 2017 (58)
- ▶ 2016 (63)

.net
android
binary
crackme
ctf
debug
docker
drones
enll
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc



Hope you'll find it usefull.

More cases (for CVE lovers.):

- 01
- 02
- 03

See you next time!

Cheers

Posted by [code16](#) at 15:28



Labels: [debug](#), [infrastructure](#), [notes](#), [pentest](#), [web](#), [writeup](#)

Brak komentarzy:

Prześlij komentarz



Wpisz komentarz



pwn
RE
web
writeup

[Nowszy post](#)

[Strona główna](#)

[Starszy post](#)

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