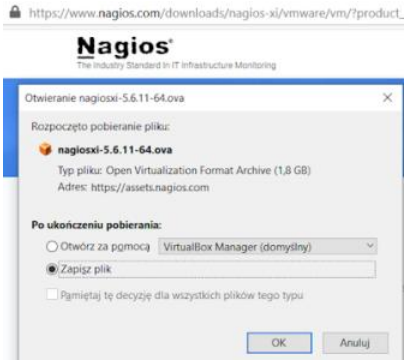
ŚRODA, 11 MARCA 2020

Nagios 5.6.11 XSS'd

Because today most of time I was in a train... most of time I spent on checking latest Nagios XI (5.6.11) VM. :) Below you will find few notes about it. Here we go...
Today we'll start here:



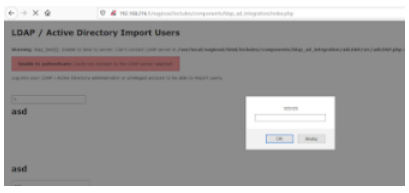
TL;DR:

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:

#01 - /ldap_ad_integration/: username parameter:

Response (src):

Presented in browser:



Little hint from the source code:

#02 - same link, param: password - similar story:

#03 - /account/main.php: theme:

O MNIE

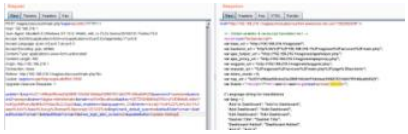
code16
Cody Sixteen
Wyświetl mój pełny profil

ARCHIWUM BLOGA

► 2022 (16)
► 2021 (37)
▼ 2020 (62)
► 12 (1)
► 11 (2)
► 10 (1)
► 09 (2)
► 08 (5)
► 07 (5)
► 06 (7)
► 05 (5)
► 04 (11)
▼ 03 (10)
Pentesting Zen Load Balancer - quick tutorial
Creating poc for preauth Symantec Web Gateway RCE
Postauth RCE in Symantec Web Gateway
Creating poc for NagiosXI 0day
Postauth RCE in ManageEngine 14
Postauth RCE bugs in NagiosXI 5.6.11
Postauth SQLi in latest NagiosXI 5.6.11
Nagios 5.6.11 XSS'd
RCE in Artica 4.26
Playing games with Games
► 02 (6)
► 01 (7)
► 2019 (97)
► 2018 (67)
► 2017 (58)
► 2016 (63)

ETYKIETY

.net
android
binary
crackme
ctf
debug
docker
drones
enlil
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

Nowszy post | Strona główna | Starszy post

Subskrybuj: Komentarze do posta (Atom)

pwn
RE
web
writeup