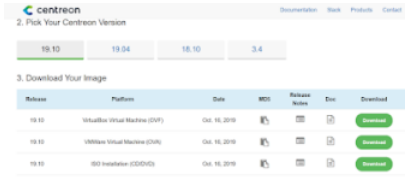
PONIEDZIAŁEK, 24 LUTEGO 2020

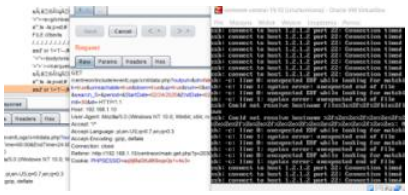
Postauth RCE in Centreon 19.10

Few hours ago I decided to check latest version of Centreon Monitoring Tool (19.10). Below you will find few notes from the journey. Here we go...
Today we will start here:

I downloaded 'latest available version' (of VM):



After a while I decided to check log files of webserver (sometimes we can find interesting *hints* there;)):



Hm... ;] Looks interesting, isn't it? ;)

Next step:

Still nothing...

When I was looking for the reason, this line appeared in the log file:

Well... ;] Again Neo!

Good! We got it. ;] So the last stage was to prepare a valid reverse shell. I used base64'd version of one of the bash-oneliners

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)
▼ 02 (6)
Postauth RCE in Centreon 19.10 - part 2
Postauth RCE in Centreon 19.10
Bug bounty scam program
Exploiting Dolibarr 11
Escaping from the Fort - quick CVE-2017-14187 autopsy
Trying harder...
► 01 (7)
► 2019 (97)
► 2018 (67)
► 2017 (58)
► 2016 (63)

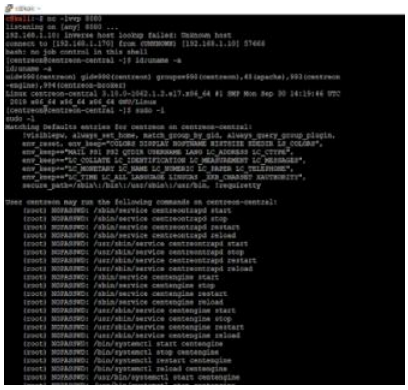
ETYKIETY

.net
android
binary
crackme
ctf
debug
docker
drones
enlil
FortiGate
fuzz
infrastructure
malware
notes
pentest
poc
pwn
RE
web
writeup

available here.

Checking:

If you are looking for a root - try here:



Maybe you'll find it useful. ;)

See you next time.

Cheers

Posted by code16 at 14:18

Labels: ctf, notes, poc, pwn, web, writeup

4 komentarze:

super 24 lutego 2020 23:41
Wow, really good one
Odpowiedz

Odpowiedzi

code16 25 lutego 2020 00:40
@super: thanks for watching;) tbh it was pretty fast one, from vm download to rce in ~3h... ;)

Odpowiedz

super 25 lutego 2020 00:48
impressive man, ive been finding some stuff here and there (not RCEs lol), wanna chat a bit about vuln research?
Odpowiedz

Odpowiedzi

code16 25 lutego 2020 06:15
@super: thanks, but no. I'm too shy. ;)

Odpowiedz

Wpisz komentarz

Motyw Okno obrazu. Obsługiwane przez usługę Blogger.