PONIEDZIAŁEK, 9 MARCA 2020

RCE in Artica 4.26

Last time I found RCE bug in an old Artica Proxy. This time I decided to check the latest one. Below you will find few results. Here we go...
Today we will start here:

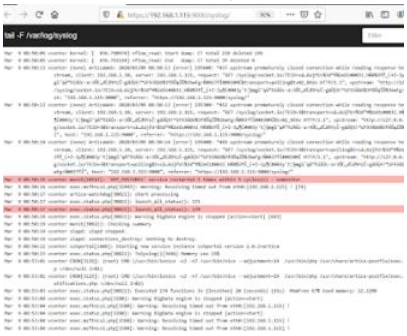
TL;DR

Yep, this is postauth RCE so to continue you'll need password of the admin user (in this case - "*Manager*").

As you will see below to achieve RCE in latest version we need to go to the Dashboard (as logged-in admin user) and click 'Change' to change the hostname, like this:

Cool. But you won't see your *asd3* file in /tmp/ now. ;)

(Just like before I opened log files to see if there will be a hint for me ;)

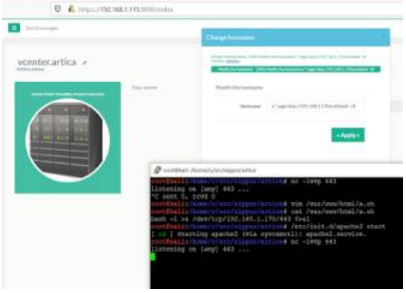


)

To get things done, now you need to go to the *DNS -> Hosts file* and *Build the file*. Remember that you'll need to wait a little bit for the application to refresh (after each of those requests). Approximate time to get a shell when you have a valid credentials is 60 seconds.

Next I decided to use some oneliner. The case was I couldn't use a quick (and valid one) so I prepared a bash-oneliner as a shell-script (in my Kali/Apache server). Next thing was to *wget* it and run with bash -interactive ;]

So:



Hostname is edited so now it's time to "Build the file" ;) Let's do it (with netcat listening on port 443):

O MNIE

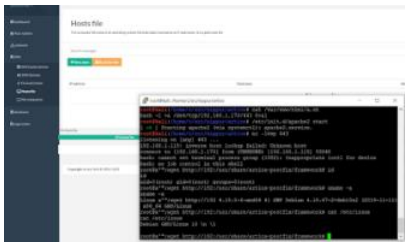
code16
Cody Sixteen
Wyświetl mój pełny profil

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



I think that's all for now. ;)

See you next time!

Cheers

** working poc will be disclosed only to patronite/donate users ;)

...but I believe it's pretty simple to write it if you want it... ;>

Posted by code16 at 07:38

Labels: notes, poc, pwn, web, writeup

Brak komentarzy:

Prześlij komentarz

Wpisz komentarz

Nowszy post Strona główna Starszy post

Subskrybuj: Komentarze do posta (Atom)

pwn

RE

web

writeup