**南开大学**

**实习实训漏洞复现报告**

**2024年7月25日**

目录

[1.漏洞复现结论（15分） 1](#_Toc28487)

[1.1风险等级分布 1](#_Toc7481)

[2.工作计划（25分） 1](#_Toc24528)

[2.1工作人员 1](#_Toc13939)

[2.2漏洞对象 1](#_Toc3137)

[2.3漏洞复现阶段 1](#_Toc7909)

[2.4风险等级 2](#_Toc1860)

[3.漏洞复现过程（35分） 2](#_Toc6133)

[3.1 风险管理及规避 2](#_Toc18532)

[3.2测试方法 2](#_Toc4033)

[3.3测试中所用的工具 2](#_Toc28445)

[4. 漏洞复现结果（25分） 3](#_Toc12892)

[4.1 POC插件编写 3](#_Toc32666)

[4.2 漏洞信息 3](#_Toc25120)

# 1.漏洞复现结论（15分）

南开大学15小组的安全人员采用科学的漏洞复现步骤于2024年7月15日至2024年7月25日对Apache Solr远程代码执行漏洞进行了全面深入的漏洞复现。

本次共发现漏洞1个，其高危漏洞1个，中危漏洞0个,低危漏洞0个。

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险值** |
| 1 | Apache Solr远程代码执行漏洞（CVE-2019-12409） | 高危 |

## 

## 1.1风险等级分布

本次评估漏洞的详细风险等级分布如下：

高危

# 2.工作计划（25分）

## 2.1工作人员

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 职务 | 姓名 | 联系方式 |
| 1 | 组长 | 常欣然 | 1195108945@qq.com |
| 2 | 组员 | 高玉格 | 1463948484@qq.com |
| 3 | 组员 | 马浩博 | 1191173636@qq.com |
| 4 | 组员 | 宋常秀 | 3281405348@qq.com |
| 5 | 组员 | 曹瑜 | 463246828@qq.com |

## 2.2漏洞对象

Apache Solr

## 2.3漏洞复现阶段

|  |  |
| --- | --- |
| 项目阶段 | 工作内容 |
| 配置环境 | 实现Docker镜像搭建 |
| 漏洞利用 | 使用msfconsole对漏洞进行利用 |
| 执行命令 | 执行任意攻击命令 |

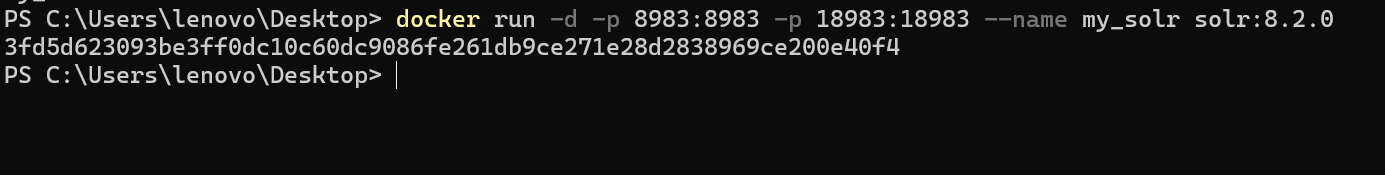
## 

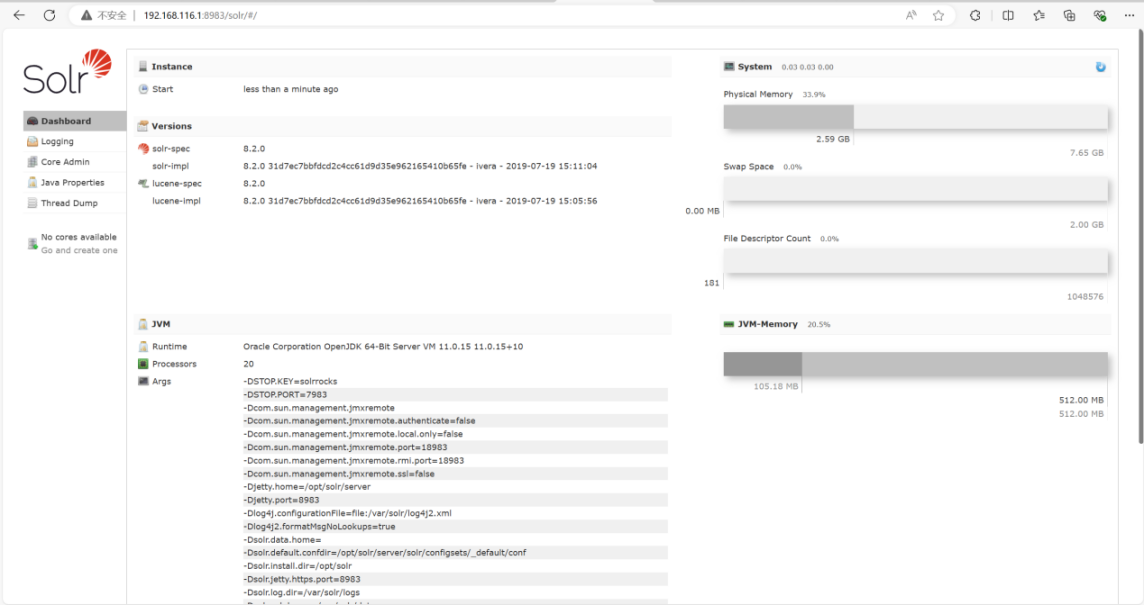
## 2.4风险等级

|  |  |  |
| --- | --- | --- |
| 编号 | 风险等级 | 风险描述 |
| 1 | 高危 | 攻击者利用此漏洞，可造成远程代码执行 |

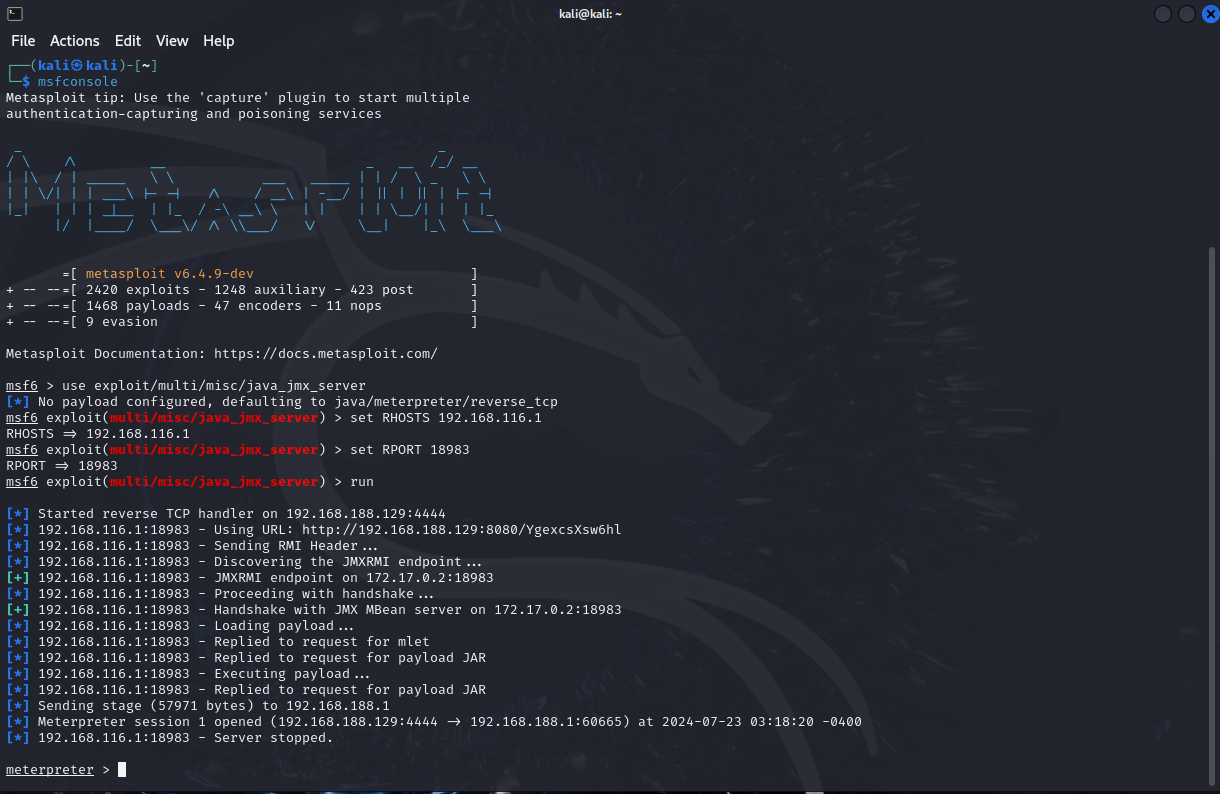
# 3.漏洞复现过程（35分）

1.1 Docker镜像搭建：docker pull solr:8.2.0。开启docker镜像，版本为solr 8.2.0。将8983和18983端口映射到本机，其中8983为solr服务端口，18983为RMI端口（漏洞利用端口）



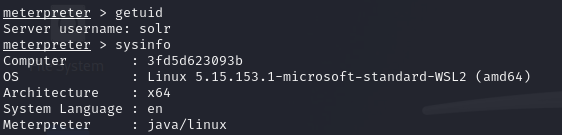


2.1使用msfconsole对漏洞进行利用。攻击成功后，建立了反向TCP连接，并获得了Meterpreter会话。



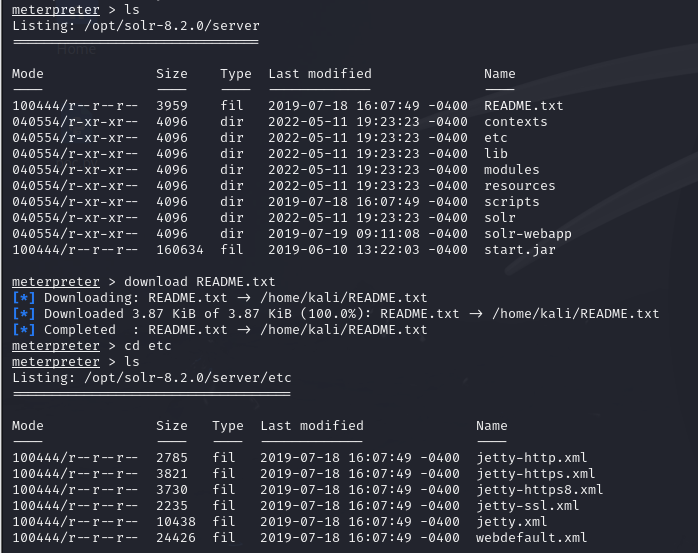
3.1尝试执行命令：

获取用户名称：solr，获取系统详细信息sysinfo



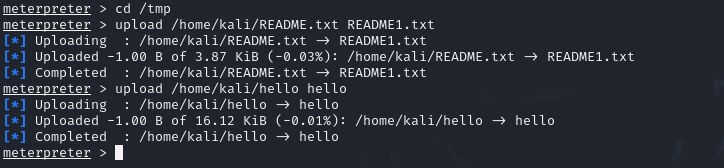
3.2查看靶机服务器本地文件，并且能够成功下载到攻击机本地（README.txt）。

能够进入其他任意文件夹查看文件

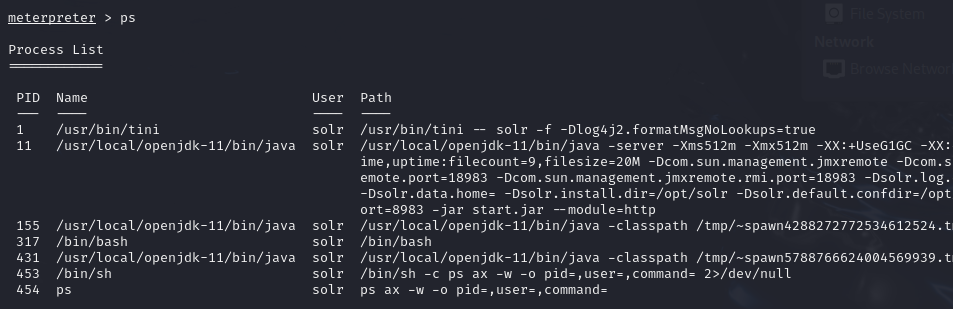


3.3甚至能够上传任意文件（需要在有写权限的文件夹下，比如tmp）

上传README.txt和可执行文件hello：



3.4 ps查看所有进程



## 3.1 风险管理及规避

（1）将Solr的solr.in.sh的ENABLE\_REMOTE\_JMX\_OPTS改为false，然后重启Solr。

（2）确认Solr管理员界面的“Java Properties”中无 com.sun.management.

jmxremote相关属性。

（3）限制Solr的公网访问，仅允许可信流量通信。

## 3.2测试方法

Poc验证

## 3.3测试中所用的工具

Docker 26.1.4

Kali 2024.2

Solr 8.2.0

# 漏洞复现结果（25分）

## 4.1 POC插件编写

poc\_CVE-2019-12409

## 4.2 漏洞信息

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** | 远程代码执行（Remote Code Execution, RCE） | **CVE-ID** | CVE-2019-12409 |
| **披露/发现时间** | 2019- 11-18 | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** | 2019-7-22 | **漏洞发现者** | Apache Solr官方 | **CNVD-ID：** |  |
| **漏洞等级** | 高危 | **提交者** | Apache Solr官方 | **搜索关键词** | Apache Solr远程代码执行 |
| **影响范围** | 受影响版本：  ApacheSolr 8.1.1  ApacheSolr 8.2.0  注：该漏洞仅对Linux系统的Solr有影响，在Windows系统中不受影响。 | | | | |
| **来源** | Apache Solr官方 | | | | |
| **漏洞简介** | 在开放的端口上，利用 javax.management.loading.MLet的getMBeansFromURL 方法来加载一个远端恶意的 MBean，可以造成远程代码执行 | | | | |
| **漏洞详情** | ApacheSolr8.1.1版本和8.2.0版本中存在安全漏洞，此漏洞因solr.in.sh配置文件中的ENABLE\_REMOTE\_JMX\_OPTS配置项默认为开启导致存在安全风险。如果使用受影响Solr版本中的默认solr.in.sh配置文件，那么将启用JMX监视并将其公开在RMI端口上（默认为18983），且无需进行任何身份验证。如果防火墙中的入站流量打开了此端口，则只要具有Solr节点网络访问权限就能够访问JMX，并且攻击者可利用该漏洞向Solr服务器上传恶意代码。 | | | | |
| **参考链接** | <https://my.f5.com/manage/s/article/K23720587>  <https://github.com/DrunkenShells/Disclosures/tree/master/CVE-2019-12409-RCE%20Vulnerability%20Due%20to%20Bad%20Defalut%20Config-Apache%20Solr>  <https://lists.apache.org/thread/7lrgowmvf144rn69ffrnd96xkgl8tw1l>  <https://lists.apache.org/thread/ryvytlrl87pjsb1csk9r1hfxhh07s7q5>  <https://lists.apache.org/thread/96zvbf9hd5ww7z1p1tpskth3qczq01nz>  <https://lists.apache.org/thread/4ztw4tvgvh03ofjsxy7pm24m3l0y1o1q>  <https://lists.apache.org/thread/d2nyofh34vdnvqzdj30wmbos19nmj8j3> | | | | |
| **靶场信息** | Solr 8.2.0 | | | | |
| **POC** | poc\_CVE-2019-12409.py | | | | |
| **修复方案** | 1.将Solr安装目录/bin文件夹下的solr.in.sh 配置文件中的“ENABLE\_REMOTE\_JMX\_OPTS”="true"配置项改为 “false”，然后重启Solr。  2、同时，应确认在Solr的管理员界面中的“Java Properties”选项中不包含 “com.sun.management.jmxremote”的相关属性信息。  3、限制Solr的公网访问，只允许可信流量与Solr建立通信。 | | | | |