Apache log4j2 远程代码执行漏洞

应急处置指南

目录

前言：背景介绍

Apache log4j2 是一款 Java 日志框架，是 log4j 的升级版。可以控制每一条日志的输出格式。通过定义每一条日志信息的级别，能够更加细致地控制日志的生成过程。

一、 如何自查是否有 log4j2 组件?

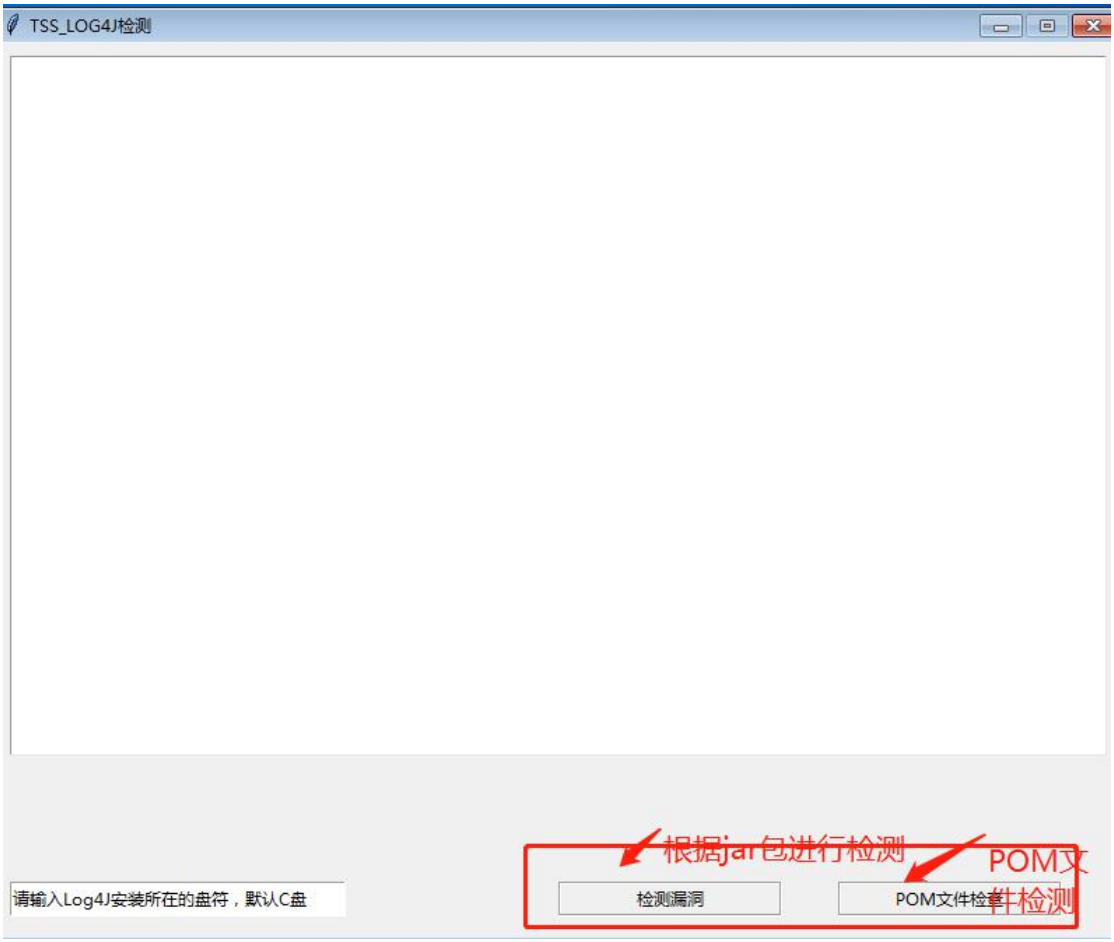
1.1 Windows 操作系统自查

- **自检工具方式**

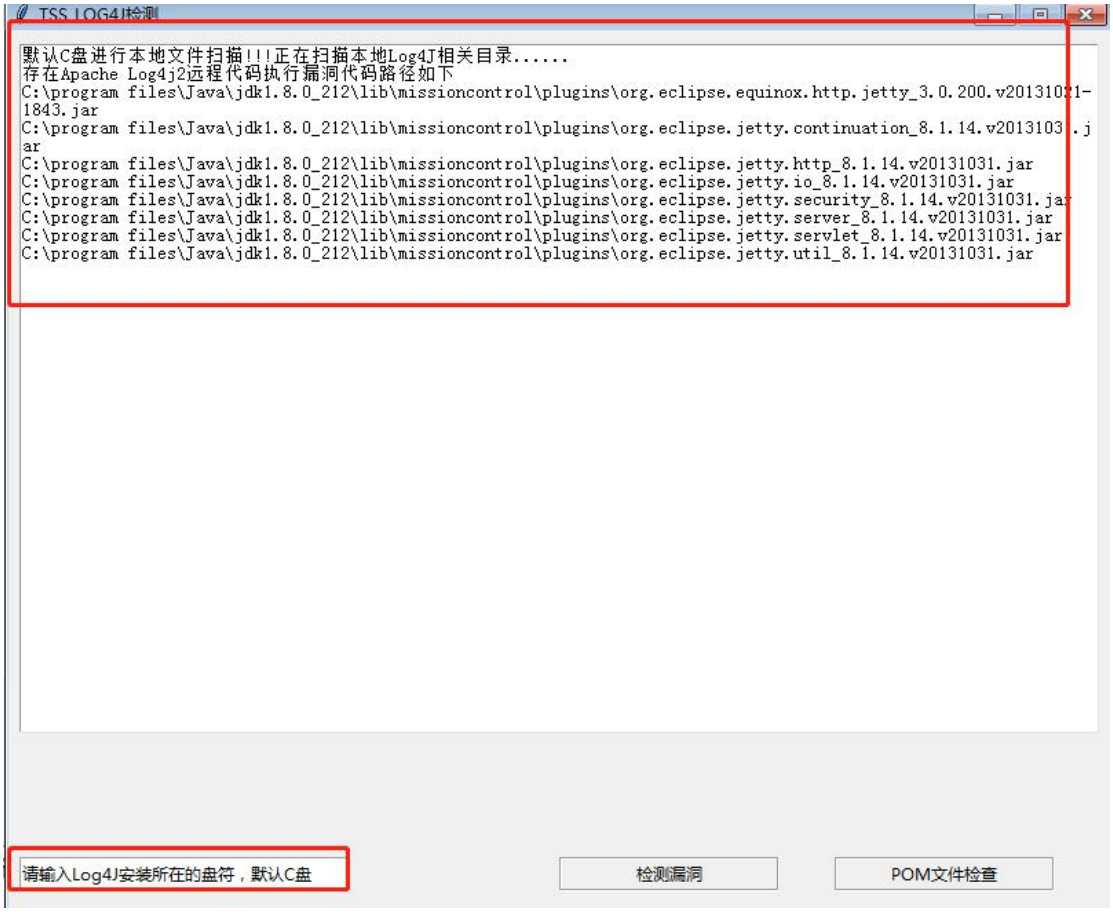
步骤一：获取自检工具“TSS-LOG4J 本地检测工具”。

请联系网络与信息中心获取此工具。

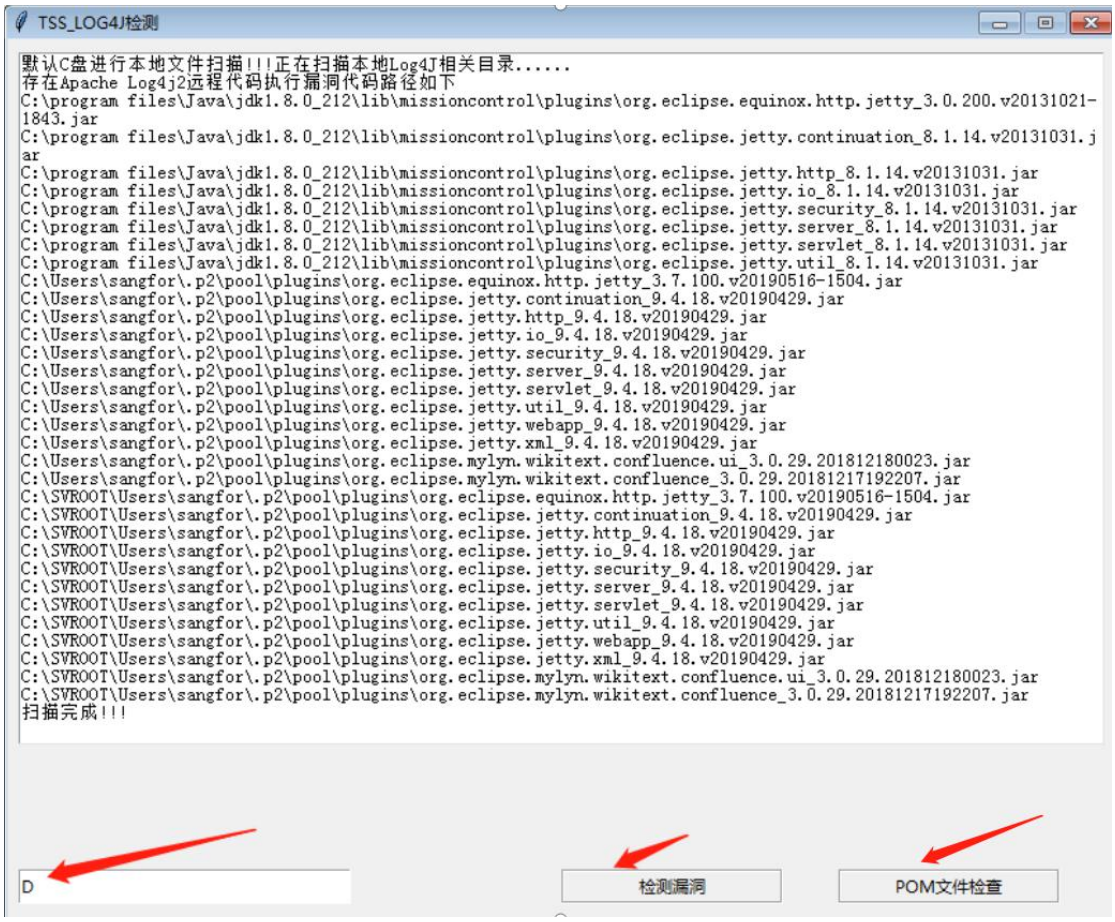
步骤二：双击打开自检工具“TSS-LOG4J 本地检测工具”，双击 exe 文件即可。



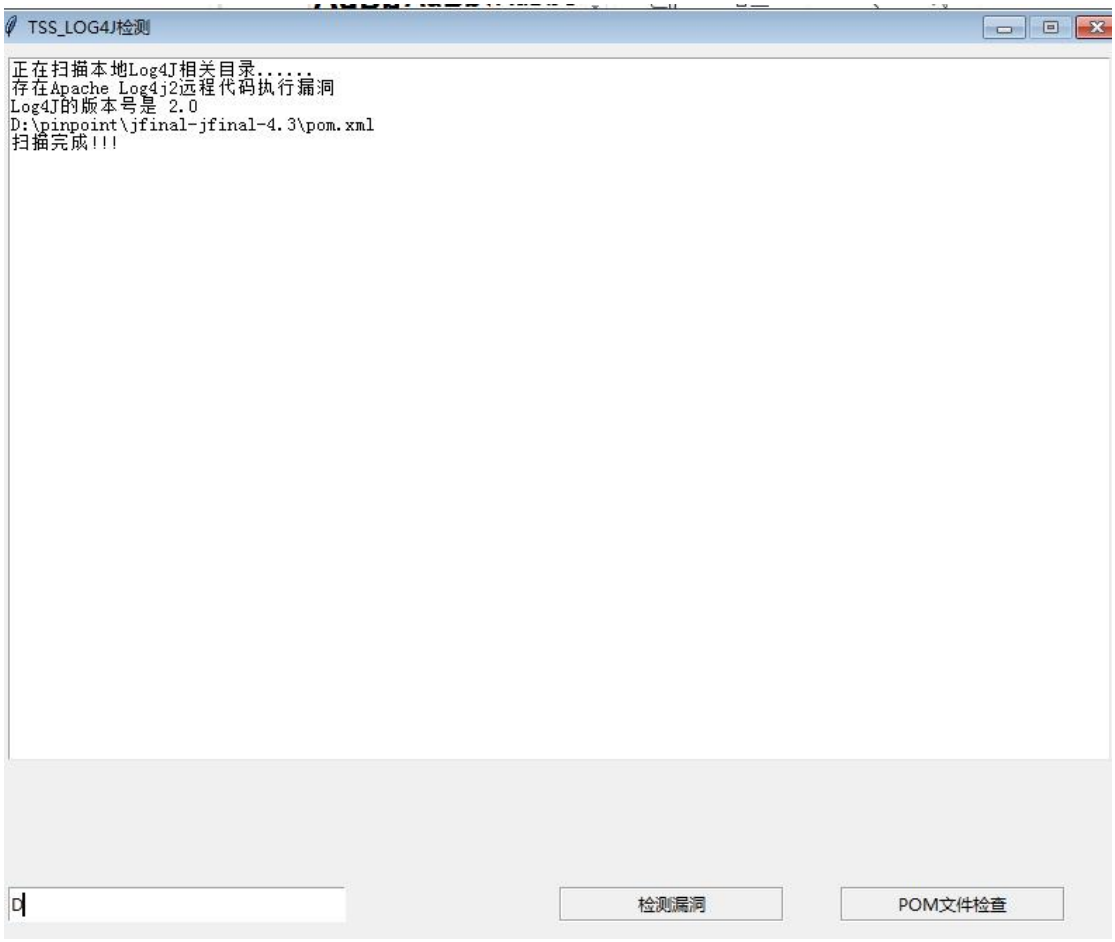
步骤三：点击检测漏洞，默认是检测 C 盘目录下的所有可能的存在漏洞的组件和版本，POM 文件检测则是检测到依赖的 Log4J 存在漏洞版本区间则停止。



支持输入特定盘符进行检测，每次只能输入一个盘符，之所以这样做是因为要保证速度，虽然代码里面已经开了多线程，但是如果一次扫描所有盘符，则等待的时间很久，交互上不太好。


TSS_LOG4J检测
默认C盘进行本地文件扫描!!!正在扫描本地Log4J相关目录.....
存在Apache Log4j2远程代码执行漏洞代码路径如下
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.equinox.http.jetty_3.0.200.v20131021-1843.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.continuation_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.http_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.io_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.security_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.server_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.servlet_8.1.14.v20131031.jar
C:\program files\Java\jdk1.8.0_212\lib\missioncontrol\plugins\org.eclipse.jetty.util_8.1.14.v20131031.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.equinox.http.jetty_3.7.100.v20190516-1504.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.continuation_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.http_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.io_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.security_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.server_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.servlet_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.util_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.webapp_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.xml_9.4.18.v20190429.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.mylyn.wikitext.confluence.ui_3.0.29.201812180023.jar
C:\Users\sangfor\.p2\pool\plugins\org.eclipse.mylyn.wikitext.confluence_3.0.29.20181217192207.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.equinox.http.jetty_3.7.100.v20190516-1504.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.continuation_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.http_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.io_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.security_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.server_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.servlet_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.util_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.webapp_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.jetty.xml_9.4.18.v20190429.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.mylyn.wikitext.confluence.ui_3.0.29.201812180023.jar
C:\SVROOT\Users\sangfor\.p2\pool\plugins\org.eclipse.mylyn.wikitext.confluence_3.0.29.20181217192207.jar
扫描完成!!!
D
检测漏洞
POM文件检查

点击进入 D 盘扫描



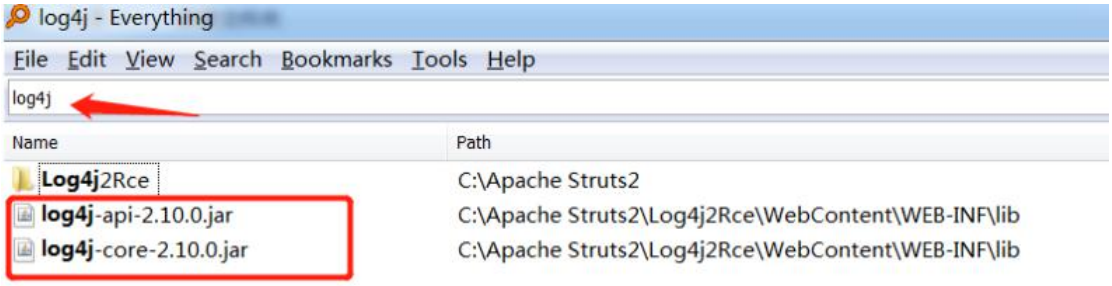
- **手工自查方式**

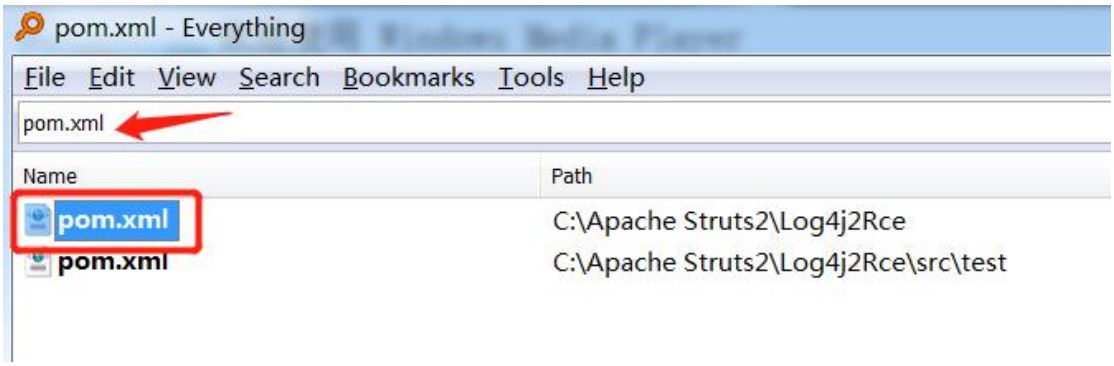
步骤一：下载全盘检索文件的工具“everything”。

请联系网络与信息中心获取此工具。

工具说明：本工具仅为方便服务器管理员在本地检索是否存在相关组件的一个快捷的方式。

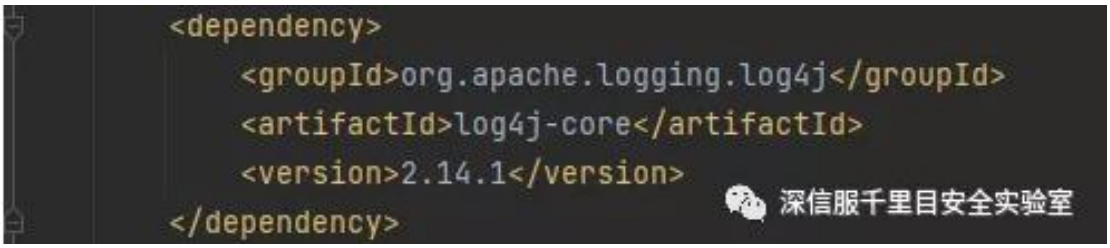
步骤二：打开“everything”工具，检索关键词“log4j”，如检索 log4j 没发现有检索结果，则检索“pom.xml”。





提示：若程序使用 Maven 打包，则会存在 pom.xml 配置文件。

步骤三：检索结果出来后可以打开 pom.xml 配置文件，查看项目的 pom.xml 文件中是否存在下图所示的相关字段，若版本号为 2.0.0 版本及以上且小于 2.15.0-rc2，则存在该漏洞。



步骤四：如以上检索均未发现结果，不能够完全下结论一定没有使用 log4j 组件，建议如果服务器有使用以下中间件的（log4j 组件通常会嵌套在以下中间件中使用），仍要联系业务系统的开发或维护厂商进行判断是否有使用 log4j 组件，如无厂商维护，则通知管理员近期保持对服务器的关注，定期做好病毒查杀和安全检查工作。

Apache log4j2 远程代码执行漏洞可能的受影响中间件包括但不限于如下：

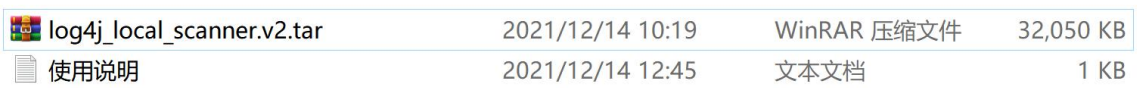
Spring-Boot-starter-log4j2
Apache Struts2
Apache Solr
Apache Flink
Apache Druid
ElasticSearch
flume
dubbo
Redis
logstash
kafka

1.2 linux 操作系统自查

- **自检工具方式**

步骤一：获取自检工具“log4j_local_scanner.v2.tar”

请联系网络与信息中心获取此工具。



步骤二：使用自检工具“log4j_local_scanner.v2.tar”，通过 jar 包内容是否包含有漏洞的 class 文件来检测。使用方式：

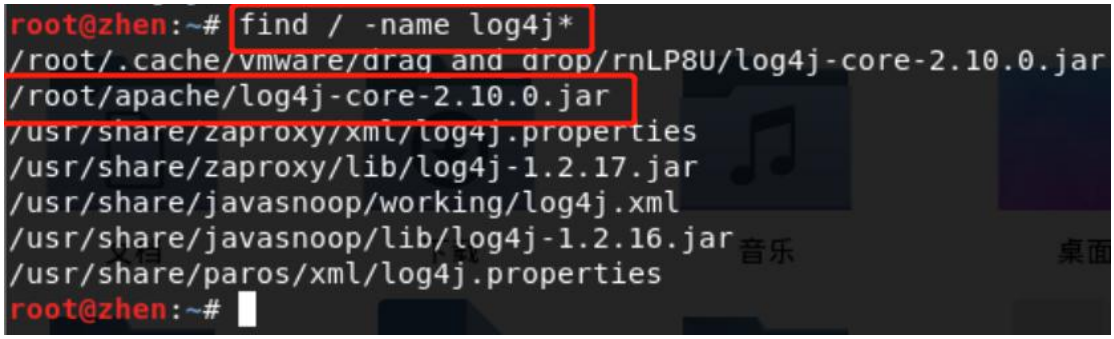
```
# 检测单个文件
```

```
sudo ./run.sh /path/to/xxx.jar/

# 检测系统所有 jar 文件

sudo ./run.sh
```

- **手工自查方式**

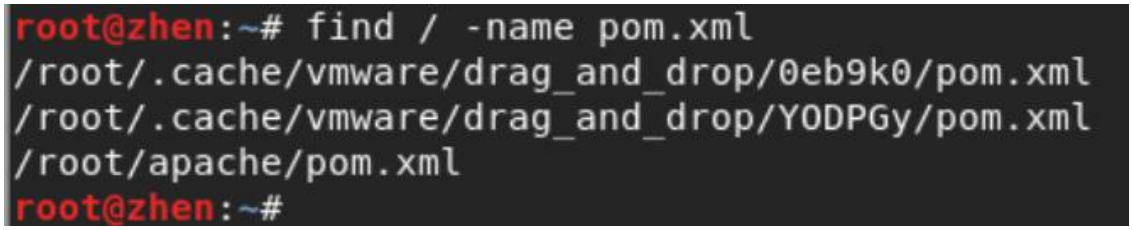
步骤一：全盘检索关键词文件“log4j”使用命令如下：

```
find / -name log4j*
```



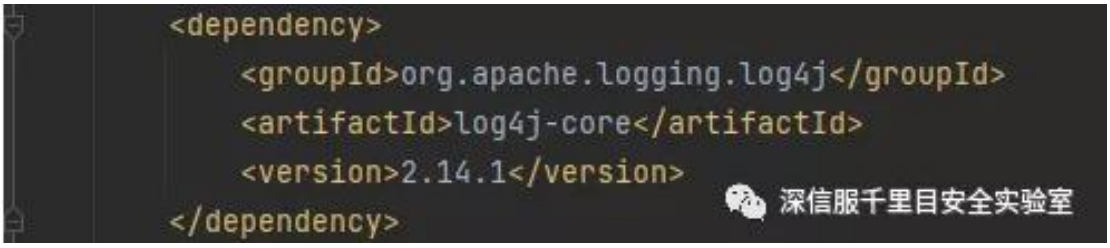
步骤二：全盘检索关键词文件“pom.xml”使用命令如下：

```
find / -name pom.xml
```



提示：若程序使用 Maven 打包，则会存在 pom.xml 配置文件。

步骤三：打开项目的 pom.xml 文件，查看 log4j-core 的 version 字段，若版本号为 2.0.0 版本及以上且小于 2.15.0-rc2，则存在该漏洞。




```
<dependency>
    <groupId>org.apache.logging.log4j</groupId>
    <artifactId>log4j-core</artifactId>
    <version>2.14.1</version>
</dependency>
```

步骤四：如以上检索均未发现结果，不能够完全下结论一定没有使用 log4j 组件，建议如果服务器有使用以下中间件的（log4j 组件通常会嵌套在以下中间件中使用），仍要联系业务系统的开发或维护厂商进行判断是否有使用 log4j 组件，如无厂商维护，则通知管理员近期保持对服务器的关注，定期做好病毒查杀和安全检查工作。

Apache log4j2 远程代码执行漏洞可能的受影响中间件包括但不限于如下：

Spring-Boot-starter-log4j2
Apache Struts2
Apache Solr
Apache Flink
Apache Druid
ElasticSearch
flume
dubbo
Redis
logstash
kafka

二、解决方案

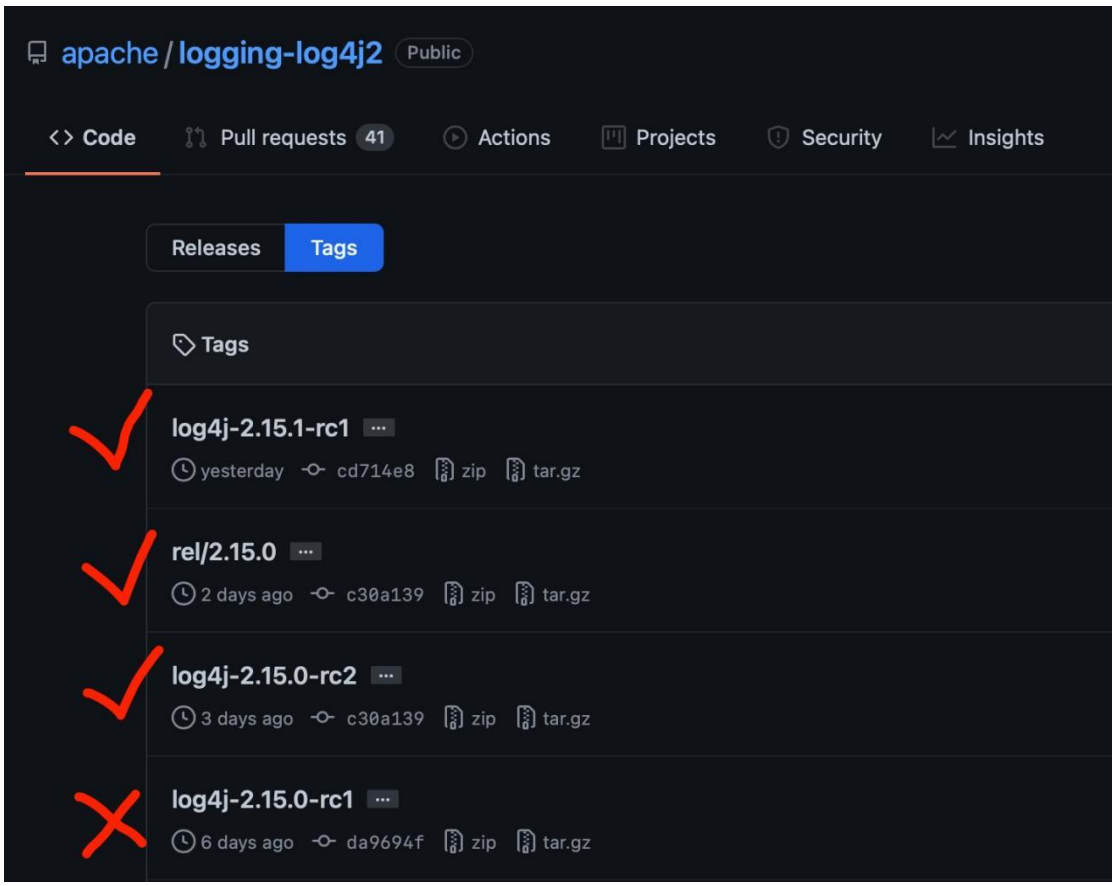
2.1 官方方案

2.1.1 升级到最新版本

注意：为了业务系统的稳定运行，log4j 组件版本的升级操作建议联系业务系统开发商或维护商升级！！否则建议采用临时缓解措施！！

升级到最新版本，版本下载链接如下：

https://github.com/apache/logging-log4j2/tags



2.1.2 临时缓解措施

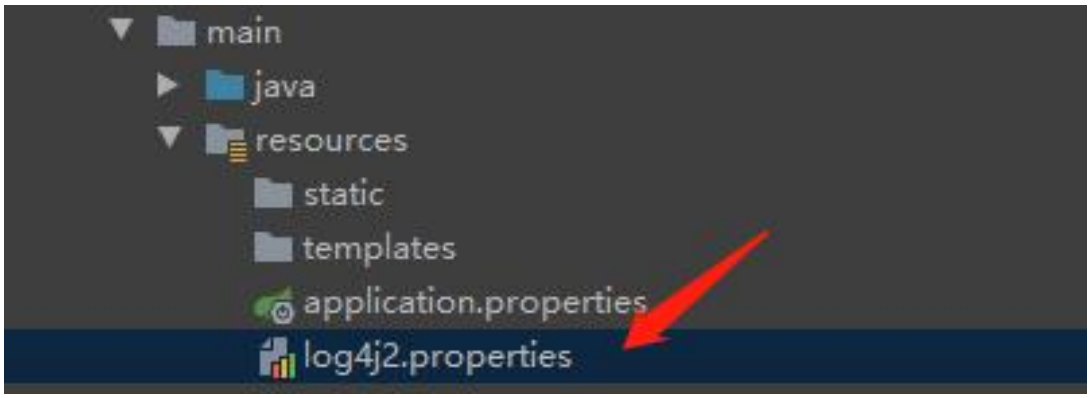
（1）在项目启动程序中添加 System.setProperty("log4j2.formatMsgNoLookups", "true");如下图所示：

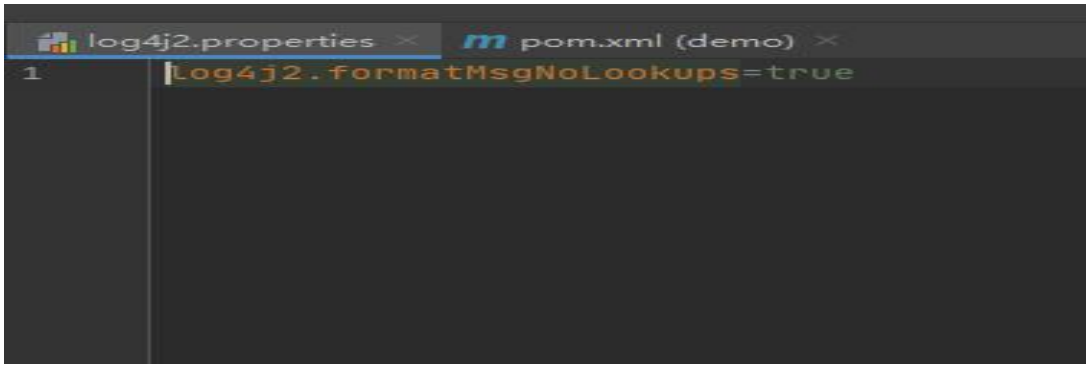
注意：因为项目启动程序具体位置和文件名均不固定，建议联系具体的开发人员找到对应的项目启动程序！！

```java
package com.example.demo;

import org.springframework.boot.SpringApplication;
import org.springframework.boot.autoconfigure.SpringBootApplication;

@SpringBootApplication
public class DemoApplication {

    static {
        System.setProperty("log4j2.formatMsgNoLookups", "true");
    }

    public static void main(String[] args) { SpringApplication.run(DemoApplication.class, args); }

}
```

（2）在应用 classpath 下添加 log4j2.properties 配置文件（文件名自定义），文件内容为：log4j2.formatMsgNoLookups=true

如图：





应急联系方式

网络与信息中心网络安全应急响应小组，QQ：1735197145