SANGFOR
深信服科技

Apache Log4j2 远程代码执行漏洞

自查手册

深信服科技股份有限公司

2021.12

目录

背景介绍

Apache Log4j2 是一款 Java 日志框架，log 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?

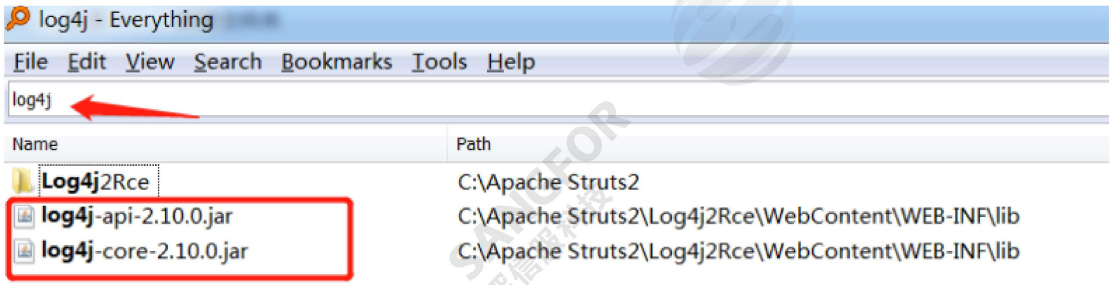
1.1 Windows 操作系统自查

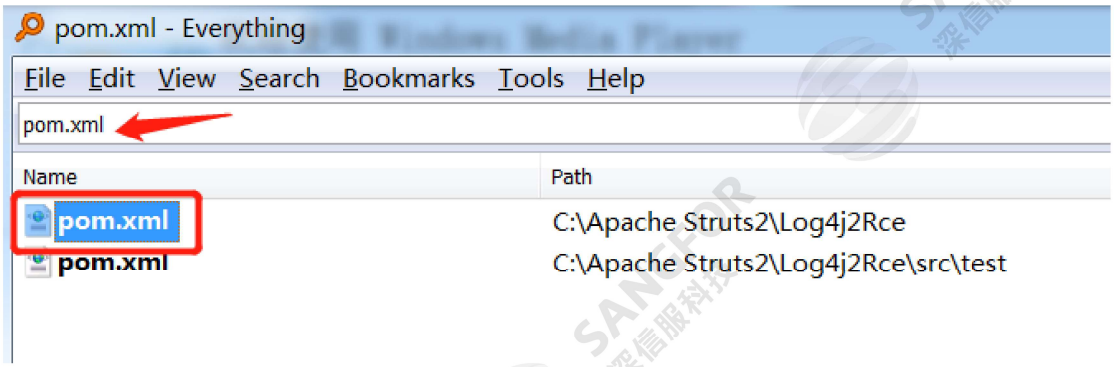
步骤一：下载全盘检索文件的工具“everything”。

请联系深信服安全服务工程师或当地技服工程师获取此工具。

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，如需要使用漏扫工具进行批量扫描可参阅文章的 2.2.1 章节。

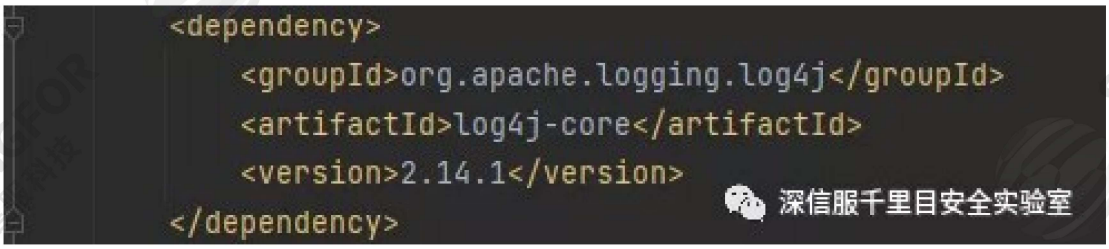
步骤二：打开“everything”工具，检索关键词“log4j”，如检索 log4j 没发现有检索结果，则检索“pom.xml”。





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并联系防火墙或 IPS 安全设备厂商更新该漏洞的防护规则库进行防护。

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

步骤一：全盘检索关键词文件“log4j”使用命令如下:

find / -name log4j*

```
root@zhen:~# find / -name log4j*
/root/.cache/vmware/drag_and_drop/rnLP8U/log4j-core-2.10.0.jar
/root/apache/log4j-core-2.10.0.jar
/usr/share/zaproxy/xml/log4j.properties
/usr/share/zaproxy/lib/log4j-1.2.17.jar
/usr/share/javasnoop/working/log4j.xml
/usr/share/javasnoop/lib/log4j-1.2.16.jar
/usr/share/paros/xml/log4j.properties
root@zhen:~#
```

步骤二：全盘检索关键词文件“pom.xml”使用命令如下:

find / -name pom.xml

```
root@zhen:~# find / -name pom.xml
/root/.cache/vmware/drag_and_drop/0eb9k0/pom.xml
/root/.cache/vmware/drag_and_drop/YODPGy/pom.xml
/root/apache/pom.xml
root@zhen:~#
```

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>
```

深信服千里目安全实验室

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并联系防火墙或 IPS 安全设备厂商更新该漏洞的防护规则库进行防护。

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

整体的解决方案共分为 4 个部分，首先是保障内网安全设备具备防护该漏洞的能力，其次是保障安全设备具备检测能力（设备**检测或服务**监测），最后如发现存在受影响版本的业务系统，则按照官方的解决方案进行修复。

2.1 防护方案

2.1.1 深信服下一代防火墙 AF

（1）确认当前设备软件升级

防火墙的【系统】-【安全能力更新】-【漏洞攻击特征识别库】需要更新到 2021-12-10 及以后版本，如下：

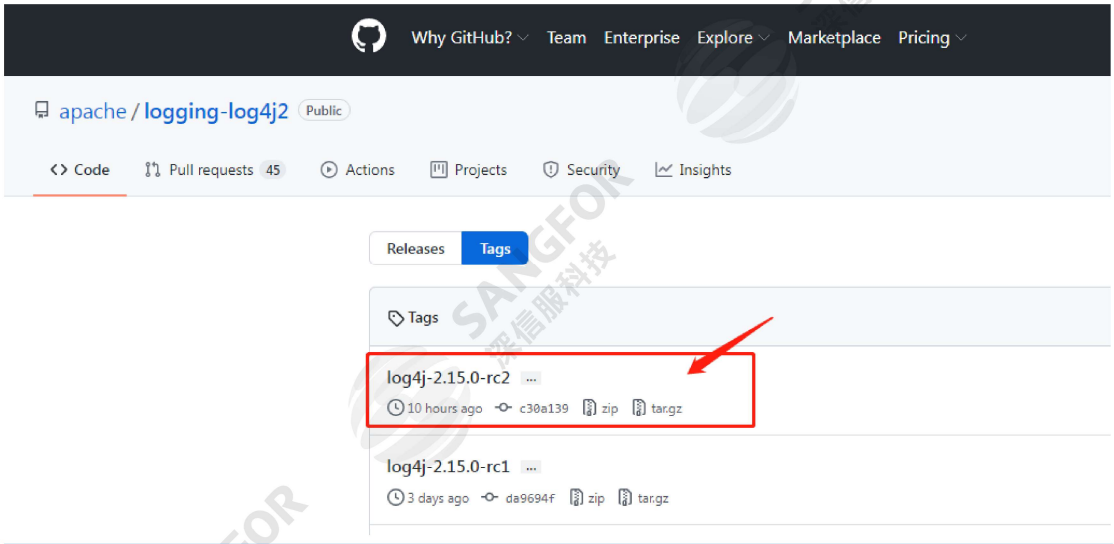
2.4 官方方案

2.4.1 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！！

(1)升级到最新版本，版本下载链接如下：

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



2.4.2 临时缓解措施

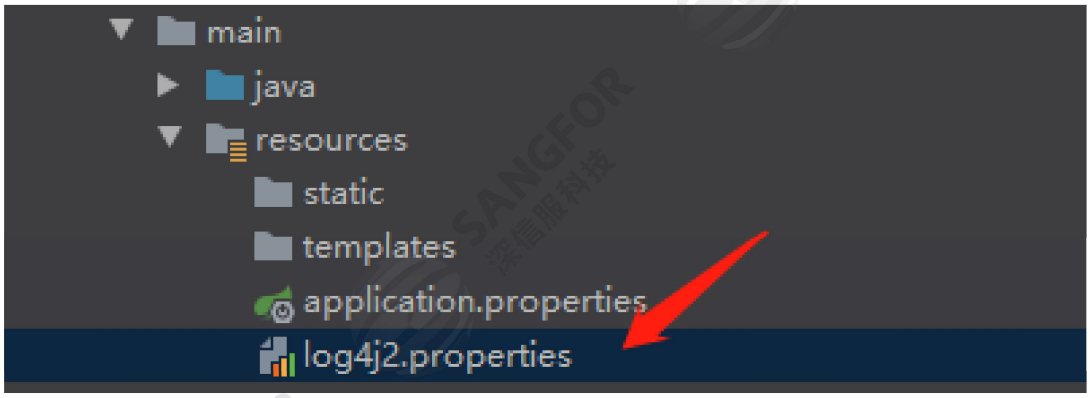
（1）在项目启动程序中添加 System.setProperty("log4j2.formatMsgNoLookups", "true");如下图所示：

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！！

```
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：



版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属深信服所有，受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可，不得以任何方式复制或引用本文的任何片断。