



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.....	3
一、 如何自查是否有 Log4j2 组件?	3
1.1 Windows 操作系统自查	3
1.2 Linux 操作系统自查	5
二、 解决方案.....	7
2.1 防护方案:	7
2.2 检测方案:	25
2.3 服务方案:	33
2.4 官方方案:	34
版权声明.....	36

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？

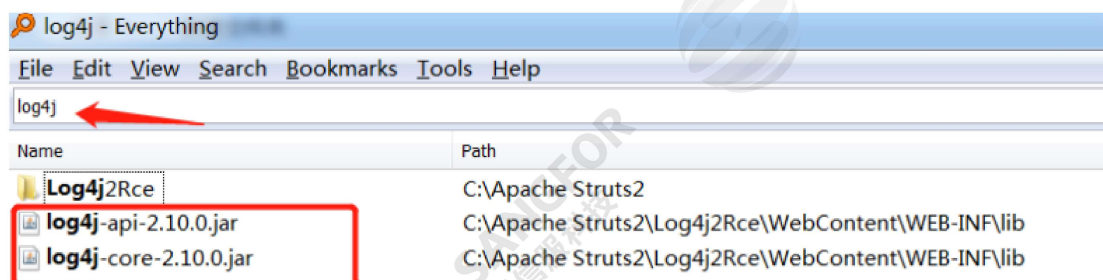
1.1 Windows 操作系统自查

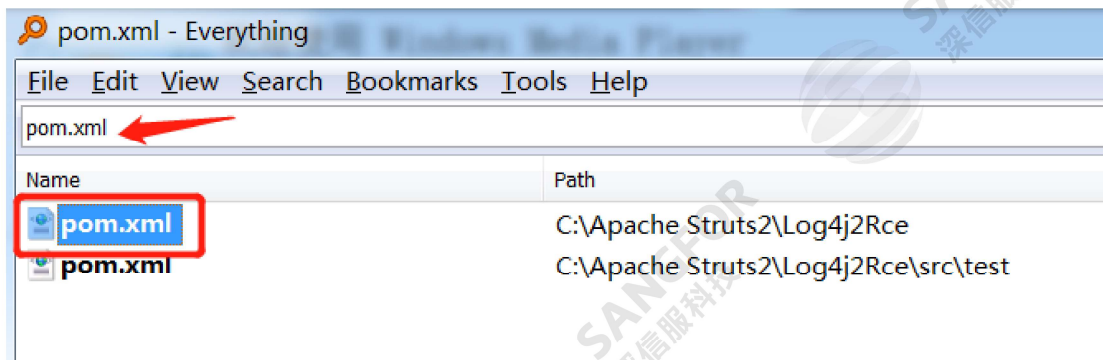
步骤一：下载全盘检索文件的工具 “everything” 。

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。

```
<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生产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/jasnoop/working/log4j.xml
/usr/share/jasnoop/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>
```

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：

深信服安全 首页 安全事件 安全漏洞 威胁情报 应急响应 安全云镜 安全工具 互动社区

严重 Apache Log4j2远程代码执行漏洞

攻击类型: 代码注入 披露时间: 更新时间: 2021-12-10
 CVE ID: CNVD ID: CNVD-2021-95914 CNVD ID: Bugtraq ID:

漏洞介绍
 该漏洞是由于Apache Log4j2某些功能存在递归解析功能, 攻击者可以利用该漏洞在未授权的情况下, 构造恶意的数据进行远程代码执行攻击, 最终获取服务器最高权限。

影响版本
 2.0 ≤ Apache Log4j ≤ 2.15.0-rc1

解决方案

- 【深信服安全运营服务】深信服云镜安全专家提供7*24小时持续的安全运营服务。在漏洞爆发之初, 云镜安全专家即对客户网络环境进行漏洞扫描, 保障第一时间检查客户的主机是否存在此漏洞。对存在漏洞的用户, 检查并更新了客户的防护设备的策略, 确保客户防护设备可以防御此漏洞风险。
- 【深信服云镜】在漏洞爆发之初, 已完成检测更新, 对所有用户网站检测, 保障用户安全。不清楚自身业务是否存在漏洞的用户, 可注册深信服云镜账号, 获取30天免费安全体验。注册地址: <http://saas.sangfor.com.cn>
- 【深信服云镜】在漏洞爆发第一时间即完成检测能力的发布, 部署了云镜的用户可以通过升级来快速检测网络中是否受该高危风险影响, 避免被攻击者利用。离线使用云镜的用户需要下载离线安装包来获得漏洞检测能力, 可以连接云镜升级的用户可自动获得漏洞检测能力。不清楚自身业务是否存在漏洞的用户, 可部署深信服云镜, 及时发现存在的风险。
- 【深信服下一代防火墙】可轻松防御此漏洞, 建议部署深信服下一代防火墙的用户更新至最新的安全防护规则, 可轻松防御此高危风险。
- 【深信服安全感知平台】可检测利用该漏洞的攻击, 实时告警, 并可联动【深信服下一代防火墙等产品】实现对攻击者IP的封堵。
- 【深信服云镜】已第一时间从云端自动更新防护规则, 云端用户无需操作, 即可轻松、快速防御此高危风险。
- 官方修复建议: 当前官方已发布最新版本, 建议受影响的用户及时更新升级到最新版本。链接如下: <https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2>

* 深信服产品购买地址: <http://www.sangfor.com.cn/order/how-to-buy.html>

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>

Why GitHub? Team Enterprise Explore Marketplace Pricing

apache / logging-log4j2 Public

Code Pull requests 45 Actions Projects Security Insights

Releases Tags

Tags

log4j-2.15.0-rc2 ...
 10 hours ago c30a139 zip targz

log4j-2.15.0-rc1 ...
 3 days ago da9694f zip targz

2.4.2 临时缓解措施

(1) 在项目启动程序中添加

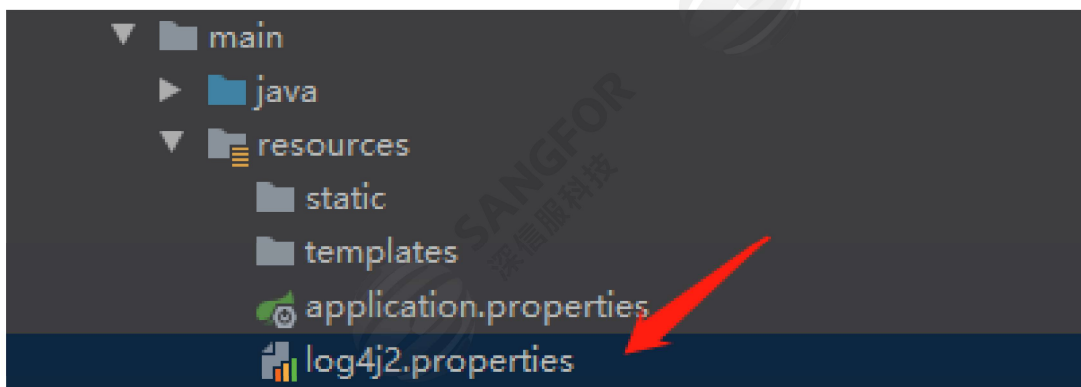
`System.setProperty("log4j2.formatMsgNoLookups", "true");`如下图所示:

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!!

```
1 package com.example.demo;
2
3 import org.springframework.boot.SpringApplication;
4 import org.springframework.boot.autoconfigure.SpringBootApplication;
5
6 @SpringBootApplication
7 public class DemoApplication {
8
9     static {
10         System.setProperty("log4j2.formatMsgNoLookups", "true");
11     }
12
13     public static void main(String[] args) { SpringApplication.run(DemoApplication.class, args); }
14
15 }
16
17
18
```

(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:



A screenshot of an IDE window showing a file named 'log4j2.properties'. The file content is:

```
1 |Log4j2.formatMsgNoLookups=true
```

 The IDE interface includes a tab for 'pom.xml (demo)' and a dark theme.

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。