网络安全风险预警通报

2022 年第 1 期 （总第 15期）

广西大学网络信息中心 2022 年 2 月 8 日

【预警类型】 高危预警

【预警内容】

Apache Log4j2 远程代码执行漏洞
漏洞风险公告

安全公告编号 CNTA-2021-0034

一、漏洞概述

Apache Log4j2 远程代码执行漏洞（CNVD-2021-95914）曝光，引发社会广泛关注。攻击者利用该漏洞，可在未授权的情况下远程执行代码，获得服务器控制权限。该漏洞具有危害程度高、利用难度低、影响范围大的特点。

二、漏洞详情

Apache Log4j 是一个基于 Java 的日志记录组件。Apache Log4j2 是 Log4j 的升级版本，通过重写 Log4j 引入了丰富的功能特性。该日志组件被广泛应用于业务系统开发，用以记录程序输入输出日志信息。

Log4j2 组件在处理程序日志记录时存在 JNDI 注入缺陷，未经授权的攻击者利用该漏洞，可向目标服务器发送精心构造的恶意数据，触发 Log4j2 组件解析缺陷，实现目标服务器的任意代码执行，获得目标服务器权限。

三、漏洞排查方法

3.1 版本排查

存在该漏洞的 Log4j2 组件版本为：Log4j2.X≤Log4j 组件版本<Log4j-2.15.0-rc2。具体组件版本排查方法如下：

（1）根据 Jar 解压后是否存在 org/apache/logging/log4j 相关路径结构，查询 Log4j2 组件及其版本情况。

（2）若程序使用 Maven 打包，查看项目的 pom.xml 文件中 org.apache.logging.log4j 相关字段及版本情况。

（3）若程序使用 Gradle 打包，可查看 build.gradle 编译配置文件，查看中 org.apache.logging.log4j 相关字段及版本情况。

3.2 中间件排查

Apache Log4j2 组件通常会嵌套在其他中间件使用，需要相关人员查看开发文档或联系系统开发商、维护人员进行判断是否有使用相关中间件。

涉及的受影响中间件或应用，包括但不限于：Apache Solr、Apache Druid、Apache Struts2、Apache Flink、Flume、Dubbo、Redis、Logstash、ElasticSearch、Kafka、Ghidra、Minecraft、Apache hive、Datax、Streaming、Dolphin Scheduler、Storm、Spring 等。

四、漏洞处置建议

4.1 官方补丁

目前，Apache 官方已发布新版本完成漏洞修复，请及时升级至最新版本 2.16.0：

https://logging.apache.org/log4j/2.x/download.html。

4.2 临时修复措施（任选其一）

（1）添加 jvm 启动参数-Dlog4j2.formatMsgNoLookups=true；

（2）在应用 classpath 下添加 log4j2.component.properties 配置文件，文件内容为 log4j2.formatMsgNoLookups=true；

（3）JDK 使用 11.0.1、8u191、7u201、6u211 及以上的高版本；

（4）限制受影响应用对外访问互联网；

（5）禁用 JNDI。

（6）部署使用第三方防火墙产品进行安全防护，并更新 WAF、RASP 规则等。