河南省教育信息安全监测中心

Apache Log4j2 远程代码执行漏洞

预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2021 年 12 月 10 日

Apache Log4j2 远程代码执行漏洞预警

事件描述

近期发现，Apache Log4j2 存在一处远程代码执行漏洞，在引入 Apache Log4j2 处理日志时，会对用户输入的内容进行一些特殊的处理，攻击者可以构造特殊的请求，触发远程代码执行。该漏洞威胁级别被定义为【严重】，影响面广泛且 POC 已公开，风险很高。

影响范围

Apache Log4j 2.x <= 2.14.1

已知受影响的应用及组件：

srping-boot-strater-log4j2/Apache Solr/Apache Flink/Apache Druid

安全建议

1、紧急缓解措施：

（1） 修改 jvm 参数 -Dlog4j2.formatMsgNoLookups=true；

（2） 修改配置 log4j2.formatMsgNoLookups=True；

（3） 将系统环境变量 FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS 设置为 true。

2、检测方案：

（1）由于攻击者在攻击过程中可能使用 DNSLog 进行漏洞探测，建议可以通过流量监测设备监控是否有相关 DNSLog 域名的请求；

（2）建议可以通过监测相关流量或者日志中是否存“jndi:ldap://”、“jndi:rmi”等字符来发现可能的攻击行为。

3、修复方案：

目前官方已发布修复版本修复了该漏洞，请受影响的用户尽快升级 Apache Log4j2 所有相关应用到最新的 log4j-2.15.0-rc1 版本。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052