【紧急】Apache Log4j任意代码执行漏洞安全风险升级修复教程

原创

Tom弹架构 于 2021-12-12 18:15:53 发布 4545 收藏 2

分类专栏： 开发工具 文章标签： java log4j 安全 安全漏洞

本文链接：https://blog.csdn.net/gupaoedu_tom/article/details/121891238

背景

近期一个 Apache Log4j 远程代码执行漏洞细节被公开，攻击者利用漏洞可以远程执行代码。经过分析，该组件存在Java JNDI注入漏洞，当程序将用户输入的数据进行日志，即可触发此漏洞，成功利用此漏洞可以在目标服务器上执行任意代码。

Apache Log4j2 是一款优秀的 Java 日志框架。该工具重写了 Log4j 框架，并且引入了大量丰富的特性。该日志框架被大量用于业务系统开发，用来记录日志信息。大多数情况下，开发者可能会将用户输入导致的错误信息写入日志中。由于 Apache Log4j2 某些功能存在递归解析功能，攻击者可直接构造恶意请求，触发远程代码执行漏洞。

经有关安全团队验证，漏洞利用无需特殊配置，Apache Struts2、Apache Solr、Apache Druid、Apache Flink等众多组件与大型应用均受影响，鉴于此漏洞危害巨大，利用门槛极低，建议用户尽快参考缓解方案阻止漏洞攻击。

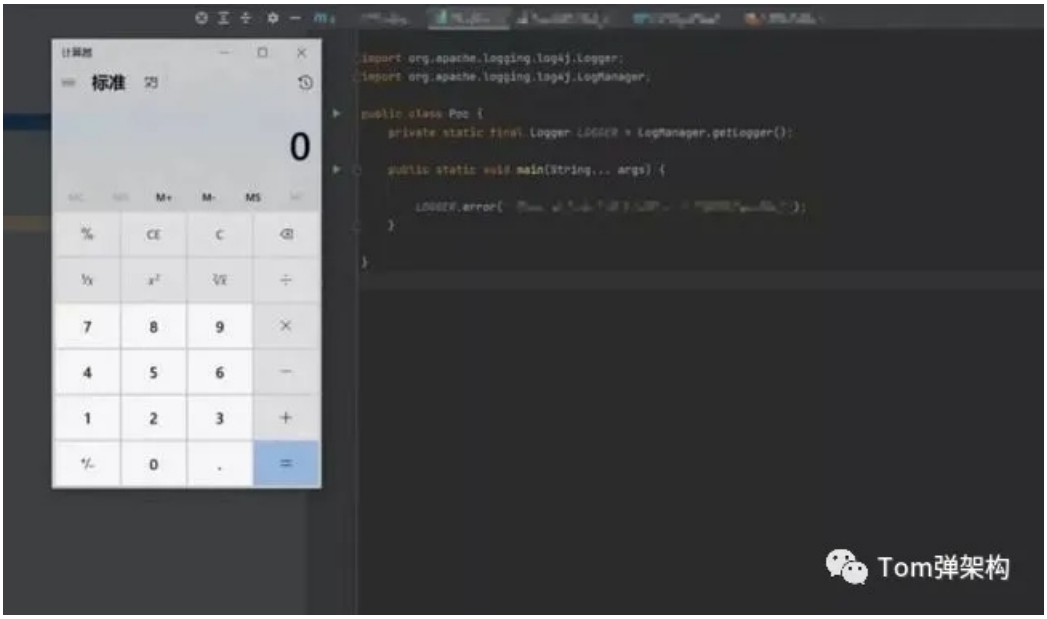
漏洞描述

事件	描述
漏洞名称	Apache Log4j 远程代码执行漏洞
漏洞类型	代码执行
风险等级	严重
公开状态	已发现

事件	描述
在野利用	已发现
漏洞描述	Apache Log4j2 是一款优秀的 Java 日志框架。该日志框架被大量用于业务系统开发，用来记录日志信息。经过分析，该组件存在Java JNDI注入漏洞，当程序将用户输入的数据进行日志，即可触发此漏洞，成功利用此漏洞可以在目标服务器上执行任意代码。
参考链接	https://github.com/apache/logging-log4j2

漏洞复现

目前漏洞rce-exp已网上公开



dnslog回显测试

易受攻击示例代码

```
import org.apache.log4j.Logger;

import java.io.*;

public class ExampleHandler implements HttpHandler {

    static Logger log = Logger.getLogger(log4jExample.class.getName());


    public void handle(HttpExchange he) throws IOException {

        String userAgent = he.getRequestHeader("user-agent");
        log.info("Request User Agent:" + userAgent);
        String response = "<h1>Hello There, " + userAgent + "!</h1>";
        he.sendResponseHeaders(200, response.length());
        OutputStream os = he.getResponseBody();
        os.write(response.getBytes());
        os.close();
    }
}
```

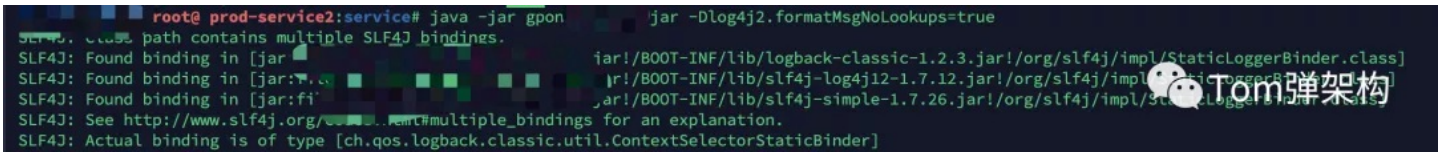
影响范围

Apache Log4j 2.x <= 2.14.1

紧急缓解措施

1、调整JVM参数 -Dlog4j2.formatMsgNoLookups=true

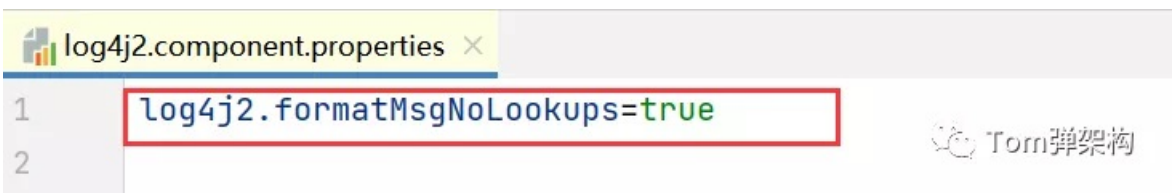
如果是SpringBoot微服务项目,在运行参数中加上



如果是传统Web项目，以Tomcat为例，在文件/bin/catalina.sh的前面，增加如下设置：

```
JAVA_OPTS='-Dlog4j2.formatMsgNoLookups=true'
```

2、修改配置 log4j2.formatMsgNoLookups=True



3、修改系统环境变量

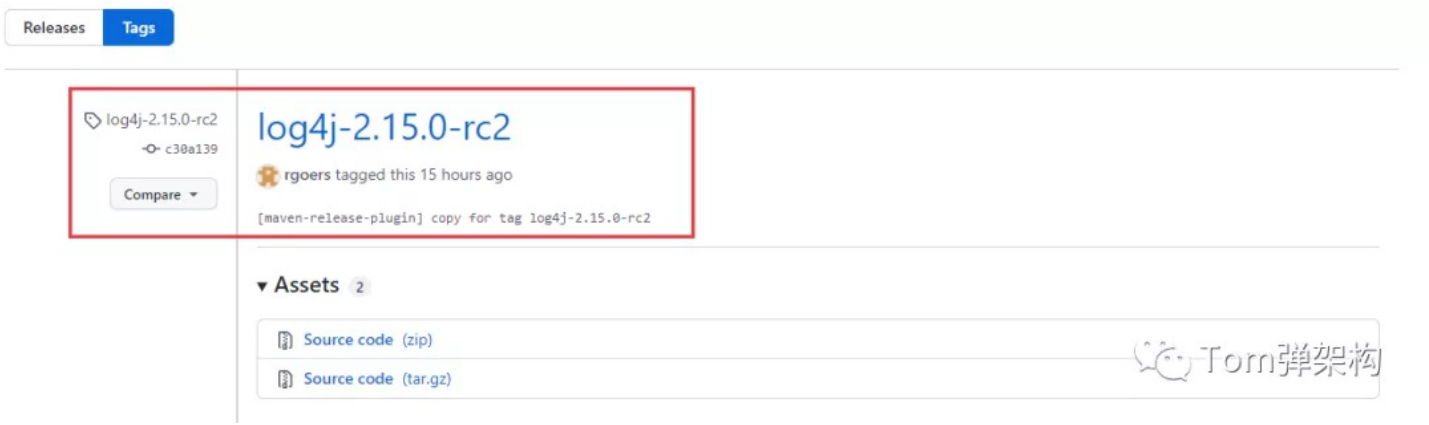
FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS 设置为true，进入Linux命令行,输入 vi /etc/profile，在最后加入

```
PATH=$PATH:$HOME/bin
export PATH
export FORMAT_MESSAGES_PATTERN_DISABLE_LOOKUPS=true
```


安全建议

1、升级 Apache Log4j2 所有相关应用到最新的 log4j-2.15.0-rc2 版本,已发现官方修复代码，目前尚未正式发布

下载地址：https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2



Github下载量巨大访问慢，可以关注回复微信公众号『 Tom弹架构 』回复“log4j” 下载最新版Log4j离线jar包。

2、升级已知受影响的应用及组件，如 srping-boot-strater-log4j2 / Apache Solr / Apache Flink / Apache Druid

据悉，Apache Log4j2 日志远程代码执行漏洞因此也影响了所有 Minecraft 服务器。

【影响版本】Apache log4j2 >= 2.0, <= 2.14.1

Minecraft 全版本所有系列服务端，除 Mohist 1.18 外。

参考资料

[1] https://github.com/apache/logging-log4j2

[2] https://github.com/apache/logging-log4j2/commit/7fe72d6

关注微信公众号『 Tom弹架构 』回复“Spring”可获取完整源码。

原创不易，坚持很酷，都看到这里了，小伙伴记得点赞、收藏、在看，一键三连加关注！如果你觉得内容太干，可以分享转发给朋友滋润滋润！