灭世之Apache Log4j2 远程代码执行漏洞

原创

TaibaiXX1 于 2021-12-11 15:38:10 发布 277 收藏
文章标签： java 大数据 python spring 人工智能

点击"仙网攻城狮”关注我们哦~

不当想研发的渗透人不是好运维

让我们每天进步一点点

简介

网上披露Apache Log4j2 远程代码执行漏洞，由于Apache Log4j2某些功能存在递归解析功能，未经身份验证的攻击者通过发送特别构造的数据请求包，可在目标服务器上执行任意代码。漏洞PoC已在网上公开，默认配置即可进行利用，该漏洞影响范围极广，建议相关用户尽快采取措施进行排查与防护。

Apache：是世界使用排名第一的Web服务器软件，可以运行在全球几乎所有广泛使用的计算机平台上。

作为Apache 的一个开源项目，Apache Log4j 2是一个基于 Java 的日志记录工具。该工具重写了 Log4j 框架，并且引入了丰富的特性，作为日志记录基础第三方库，被大量 Java 框架及应用使用。

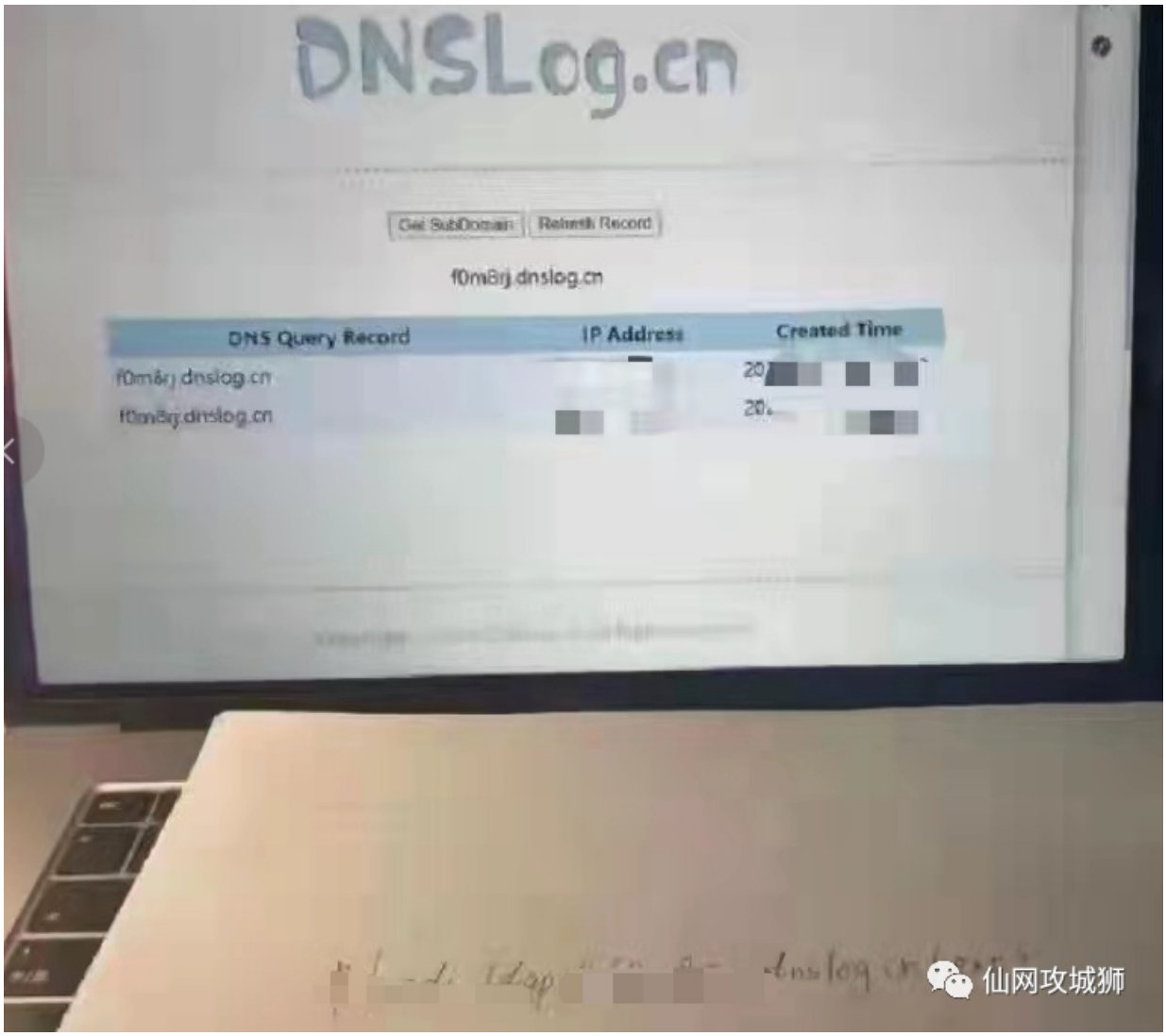
通过Google搜索引擎对依赖该组件的产品、其他开源组件分析后发现，有310个产品、开源组件依赖了Apache Log4j2 2.14.1的版本，包括诸多全球使用量的Top序列的通用开源组件，例如 Apache Struts2、Apache Solr、Apache Druid、Apache Flink等。

这个漏洞有的人称它是地震级、开源社区称它是核弹级，而我喜欢称它为灭世级，为啥称它是灭世级。看下面几个图片就明白了。

百度

iCloud

纸上触发这个就很离谱，哈哈哈



由于目前还在该漏洞的应急期（爆出漏洞之后1-2个月）还不知道payload的可以在微信公众号里面回复**“牛X”**就可以获取，直接放在文章里面怕被举报哈

高级利用骚姿势

在还有人不知所以的时候有的大佬已经研究出如何利用这个漏洞去搞物联网设备、耳机、电脑、开放WiFi的设备等，这就很离谱。

大概的利用方法就是把蓝牙名称和wifi名称加入payload即可，简单粗暴。

最后不得不提一下，昨晚最忙的可能不是安全从业者，而是 dnslog，哈哈！

往期内容

CFT学习资源与工具上新

工具篇-BurpSutie Pro 2021.10.1最新版本

2021湖北省工匠杯预赛WriteUP

更多资讯长按二维码 关注我们

觉得不错点个“赞”呗