Nexus Repository Manager 3 表达式解析漏洞复现

原创s1mp1e Timeline Sec
1970-01-01原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：s1mp1e（团队复现组成员）

本文字数：578

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

Nexus Repository 是一个开源的仓库管理系统，在安装、配置、使用简单的基础上提供了更加丰富的功能。3 月 31 日 Nexus Repository Manager 官方发布了 CVE-2020-10199 CVE-2020-10204 的漏洞通告信息，两个漏洞均是由 Github Secutiry Lab 的是 @pwntester 发现的。

0x02 漏洞概述

CVE-2020-10199 和 CVE-2020-10204 主要是由于可执行恶意 EL表达式 导致的。

0x03 影响版本

Nexus Repository Manager 3.x OSS / Pro <= 3.21.1

0x04 环境搭建

1、拉取镜像

```
docker pull sonatype/nexus3:3.21.1
```

2、创建nexus数据目录

```
mkdir /your-dir/nexus-data && chown -R 200 /your-dir/nexus-data
```

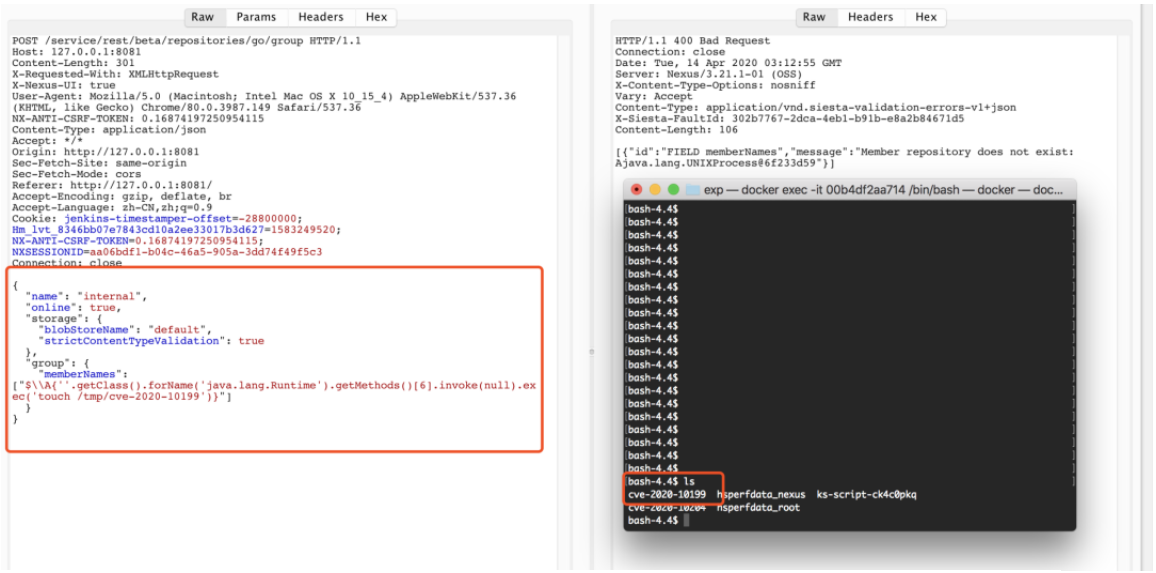
3、运行nexus docker镜像

```
docker run -d --rm -p 8081:8081 -p 5050:5050 --name nexus -v
/your-dir/nexus-data -e INSTALL4J_ADD_VM_PARAMS="-Xms2g -Xmx2g -
XX:MaxDirectMemorySize=3g  -Djava.util.prefs.userRoot=/nexus-
data -
agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=505
0" sonatype/nexus3::3.21.1
```

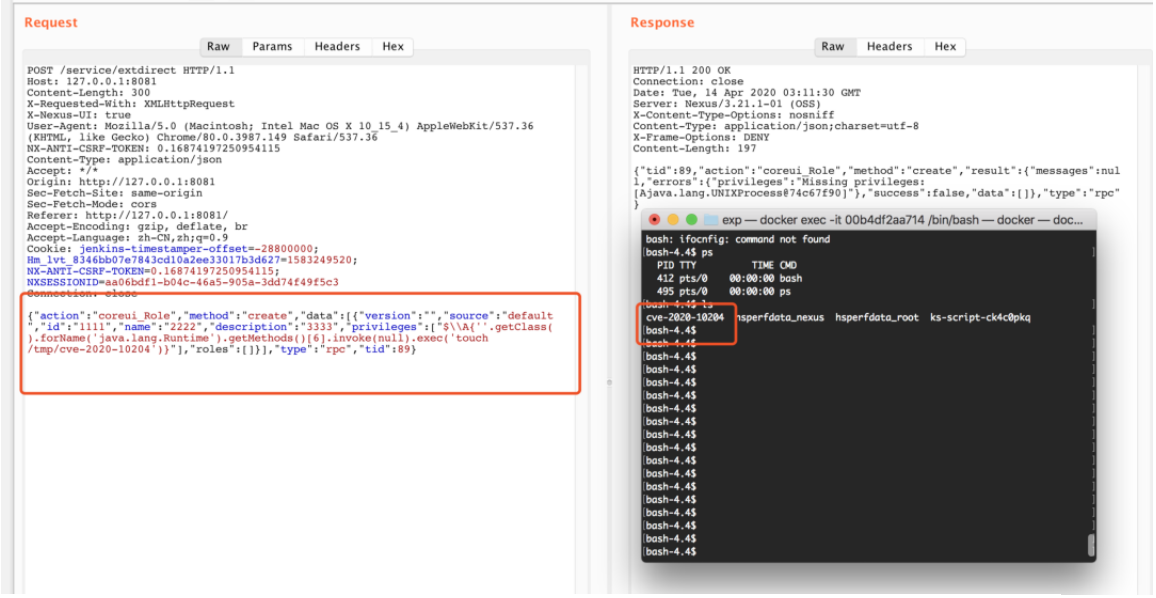
0x05 漏洞复现

参 考 链 接 中 附 下 载 地 址

CVE-2020-10199(普通用户权限)



CVE-2020-10204 （需要管理员权限）



注：需手动更改请求头中 NX-ANTI-CSRF-TOKEN=0.16874197250954115; NXSESSIONID=aa06bdf1-b04c-46a5-905a-3dd74f49f5c3 内容为本地真实环境值。

0x06 修复方式

升级至最新版本或 Nexus Repository Manager 3.x OSS / Pro > 3.21.1

参考链接：

https://www.anquanke.com/post/id/202867

https://github.com/threedr3am/learnjavabug/tree/master/nexus/CVE-2020-10199

https://github.com/threedr3am/learnjavabug/tree/master/nexus/CVE-2020-10204

原理类书籍推荐

阅读原文看更多复现文章

Timeline Sec 团队

精选留言

用户设置不下载评论

阅读全文