index : kernel/git/torvalds/linux.git

master switch

Linux kernel source tree Linus Torvalds

about summary refs log tree commit diff stats log msg search

author	Kees Cook <keescook@chromium.org>	2021-05-25 12:37:35 -0700
committer	Linus Torvalds <torvalds@linux-foundation.org>	2021-05-25 10:24:41 -1000
commit	bfb819ea20ce8bbeeba17e1a6418bf8bda91fc28 (patch)	
tree	d5327bdc0a2bb41db9968c7937810d40875b090a	
parent	ad9f25d338605d26acedcaf3ba5fab5ca26f1c10 (diff)	
download	linux-bfb819ea20ce8bbeeba17e1a6418bf8bda91fc28.tar.gz	

diff options

context: 3

space: include

mode: unified

proc: Check /proc/$pid/attr/ writes against file opener

```
Fix another "confused deputy" weakness[1]. Writes to /proc/$pid/attr/
files need to check the opener credentials, since these fds do not
transition state across execve(). Without this, it is possible to
trick another process (which may have different credentials) to write
to its own /proc/$pid/attr/ files, leading to unexpected and possibly
exploitable behaviors.

[1] https://www.kernel.org/doc/html/latest/security/credentials.html?highlight=confused#open-file-credentials

Fixes: 1da177e4c3f41 ("Linux-2.6.12-rc2")
Cc: stable@vger.kernel.org
Signed-off-by: Kees Cook <keescook@chromium.org>
Signed-off-by: Linus Torvalds <torvalds@linux-foundation.org>
```

Diffstat

-rw-r--r-- fs/proc/base.c 4

1 files changed, 4 insertions, 0 deletions

```
diff --git a/fs/proc/base.c b/fs/proc/base.c
index 3851bfcdba56e..58bbf334265b7 100644
--- a/fs/proc/base.c
+++ b/fs/proc/base.c
@@ -2703,6 +2703,10 @@ static ssize_t proc_pid_attr_write(struct file * file, const char __user * buf,
        void *page;
        int rv;

+       /* A task may only write when it was the opener. */
+       if (file->f_cred != current_real_cred())
+               return -EPERM;
+
        rcu_read_lock();
        task = pid_task(proc_pid(inode), PIDTYPE_PID);
        if (!task) {
```