Subject: [PATCH] file: Add locking to f_getown
Posted by ebiederm on Sun, 10 Sep 2006 04:11:18 GMT

View Forum Message <> Reply to Message

This has been needed for a long time, but now with the advent
of a reference counted struct pid there are real consequences
for getting this wrong.

Someone I think it was Oleg Nesterov pointed out that this construct
was missing locking, when I introduced struct pid. After taking time
to review the locking construct already present I figured out which
lock needs to be taken. The other paths that access f_owner.pid
take either the f_owner read or the write lock.

Signed-off-by: Eric W. Biederman <ebiederm@xmission.com>

```
---
 fs/fcntl.c |    2 ++
 1 files changed, 2 insertions(+), 0 deletions(-)

diff --git a/fs/fcntl.c b/fs/fcntl.c
index 821ebb9..b1dd4d4 100644
--- a/fs/fcntl.c
+++ b/fs/fcntl.c
@@ -305,9 +305,11 @@ void f_delown(struct file *filp)
 pid_t f_getown(struct file *filp)
 {
  pid_t pid;
+ read_lock(&filp->f_owner.lock);
  pid = pid_nr(filp->f_owner.pid);
  if (filp->f_owner.pid_type == PIDTYPE_PGID)
   pid = -pid;
+ read_unlock(&filp->f_owner.lock);
  return pid;
 }

--
1.4.2.rc3.g7e18e-dirty
```