
Subject: [PATCH][IPC] Lost unlock and fput in mqueue.c on error path

Posted by [Pavel Emelianov](#) on Wed, 21 Nov 2007 13:54:58 GMT

[View Forum Message](#) <> [Reply to Message](#)

The error path in sys_mq_getsetattr() after the call to audit_mq_getsetattr() is wrong - the info->lock is not unlocked and the struct file *filp is not put.

Fix them both.

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

diff --git a/ipc/mqueue.c b/ipc/mqueue.c

index 0ce1ba6..7d1b8aa 100644

--- a/ipc/mqueue.c

+++ b/ipc/mqueue.c

```
@@ -1144,8 +1144,10 @@ asmlinkage long sys_mq_getsetattr(mqd_t mqdes,
    omqstat.mq_flags = filp->f_flags & O_NONBLOCK;
    if (u_mqstat) {
        ret = audit_mq_getsetattr(mqdes, &mqstat);
-   if (ret != 0)
-       goto out;
+   if (ret != 0) {
+       spin_unlock(&info->lock);
+       goto out_fput;
+   }
    if (mqstat.mq_flags & O_NONBLOCK)
        filp->f_flags |= O_NONBLOCK;
    else
```
