Subject: [PATCH] proc: check vma->vm_file before dereferencing
Posted by Stanislav Kinsbursky on Mon, 15 Oct 2012 15:30:03 GMT
View Forum Message <> Reply to Message

It can be equal to NULL.

Signed-off-by: Stanislav Kinsbursky <skinsbursky@parallels.com>
---
 fs/proc/base.c | 5 +++--
 1 files changed, 3 insertions(+), 2 deletions(-)

```
diff --git a/fs/proc/base.c b/fs/proc/base.c
index 144a967..74fc562 100644
--- a/fs/proc/base.c
+++ b/fs/proc/base.c
@@ -1770,8 +1770,9 @@ static struct dentry *proc_map_files_lookup(struct inode *dir,
  if (!vma)
   goto out_no_vma;

- result = proc_map_files_instantiate(dir, dentry, task,
-   (void *)(unsigned long)vma->vm_file->f_mode);
+ if (vma->vm_file)
+  result = proc_map_files_instantiate(dir, dentry, task,
+    (void *)(unsigned long)vma->vm_file->f_mode);

 out_no_vma:
  up_read(&mm->mmap_sem);
```