Subject: [PATCH] /proc/*/environ: wrong placing of ptrace_may_attach() check
Posted by Alexey Dobriyan on Mon, 28 May 2007 13:33:13 GMT
View Forum Message <> Reply to Message

Signed-off-by: Alexey Dobriyan <adobriyan@sw.ru>
---

 fs/proc/base.c | 11 ++++++++---
 1 file changed, 8 insertions(+), 3 deletions(-)

```
--- a/fs/proc/base.c
+++ b/fs/proc/base.c
@@ -204,12 +204,17 @@ static int proc_pid_environ(struct task_
  int res = 0;
  struct mm_struct *mm = get_task_mm(task);
  if (mm) {
-  unsigned int len = mm->env_end - mm->env_start;
+  unsigned int len;
+
+  res = -ESRCH;
+  if (!ptrace_may_attach(task))
+   goto out;
+
+  len  = mm->env_end - mm->env_start;
   if (len > PAGE_SIZE)
    len = PAGE_SIZE;
   res = access_process_vm(task, mm->env_start, buffer, len, 0);
-  if (!ptrace_may_attach(task))
-   res = -ESRCH;
+out:
   mmput(mm);
  }
  return res;
```