

[PATCH] race condition in procfs

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-11/9370.html>

From: Grzegorz Nosek (grzegorz.nosek_at_gmail.com)

Date: 11/29/05

Date: Tue, 29 Nov 2005 08:17:22 +0100
To: linux-kernel@vger.kernel.org

Hello,

I found a race condition in procfs on SMP systems. The result is an oops in processes like pidof. Apparently `->proc_read()` gets passed a potentially NULL pointer. The following micro-patch seems to fix it.

Best regards,
Grzegorz Nosek

```
--- linux-2.6/fs/proc/base.c.orig 2005-11-25 00:07:43.000000000 +0100
+++ linux-2.6/fs/proc/base.c 2005-11-28 11:44:11.000000000 +0100
@@ -718,6 +718,9 @@
     ssize_t length;
     struct task_struct *task = proc_task(inode);

+ if (!task)
+ return -ENOENT;
+
     if (count > PROC_BLOCK_SIZE)
         count = PROC_BLOCK_SIZE;
     if (!(page = __get_free_page(GFP_KERNEL)))
-
```

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>