

---

Subject: Re: [PATCH -mm] utrace: fix double free re \_\_rcu\_process\_callbacks()  
Posted by [Alexey Dobriyan](#) on Tue, 24 Apr 2007 10:32:43 GMT

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

---

On Tue, Apr 24, 2007 at 01:10:23PM +0400, Alexey Dobriyan wrote:

- > but weren't easily reproducible without hitting double-free first.
- > FWIW, it's
- > `BUG_ON(!list_empty(&tsk->ptracees));`

mmm, pretty easily reproduced with:

```
while true; do
  killall -9 expl_ptratt 2>/dev/null;
  killall -9 exe 2>/dev/null;
  sleep 2;
done
```

vs

```
while true; do ./expl_ptratt; done
```

---