Subject: Re: utrace, RCU and ia64
Posted by Alexey Dobriyan on Tue, 17 Apr 2007 11:12:55 GMT
View Forum Message <> Reply to Message

[double freeing of struct utrace leading to oops in
 __rcu_process_callbacks]

Hi, Roland,

utrace debugging you've put into 2.6.21-rc6-mm1 helped. Two double-frees reproduced:

```
1) BUG at kernel/utrace.c:176
 rcu_utrace_free
 utrace_reap
 utrace_release_task
 release_task
 flush_old_exec
 load_elf_binary
 search_binary_handler
 do_execve

2) rcu_utrace_free
 check_dead_utrace
 remove_detached
 finish_report_death
 utrace_report_death
 do_exit
 debug_mutex_init
 get_signal_to_deliver
 do_notify_resume
 ptregscall_common
 sysret_signal
----------------
```

I've sprinkled more atomic_set's over utrace code to determine who is at fault of first freeing. It seems to be

```
 rcu_utrace_free
 check_dead_utrace
 wake_quiscent
 utrace_detach
```

It was atomic_set(&utrace->debug, 42) right before wake_quiscent() call and printk() in rcu_utrace_free() call. So it was 42 or garbage.

How I understand all this is that check_dead_utrace() can free struct utrace, and don't clear ->utrace pointer.