

---

Subject: [PATCH 1/2 (resend)] Clean up the kill\_something\_info  
Posted by [Pavel Emelianov](#) on Mon, 04 Feb 2008 13:02:02 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

This is the first step (of two) in removing the kill\_pgrp\_info.

All the users of this function are in kernel/signal.c, but all they need is to call \_\_kill\_pgrp\_info() with the tasklist\_lock read-locked.

Fortunately, one of its users is the kill\_something\_info(), which already needs this lock in one of its branches, so clean these branches up and call the \_\_kill\_pgrp\_info() directly.

Based on Oleg's view of how this function should look.

Changes from v1:

- \* Fixed double rcu\_read\_lock() in the if (pid > 0) branch.  
This caused udev die from segfault on FC3, as noticed by Andrew.

Signed-off-by: Oleg Nesterov <oleg@tv-sign.ru>

Signed-off-by: Pavel Emelyanov <xemul@openvz.org>

---

kernel/signal.c | 26 ++++++-----  
1 files changed, 15 insertions(+), 11 deletions(-)

diff --git a/kernel/signal.c b/kernel/signal.c

index cc45a6b..a805c74 100644

--- a/kernel/signal.c

+++ b/kernel/signal.c

@@ -1134,14 +1134,22 @@ EXPORT\_SYMBOL\_GPL(kill\_pid\_info\_as\_uid);

static int kill\_something\_info(int sig, struct siginfo \*info, int pid)

{

int ret;

- rcu\_read\_lock();

- if (!pid) {

- ret = kill\_pgrp\_info(sig, info, task\_pgrp(current));

- } else if (pid == -1) {

+

+ if (pid > 0) {

+ rcu\_read\_lock();

+ ret = kill\_pid\_info(sig, info, find\_vpid(pid));

+ rcu\_read\_unlock();

+ return ret;

+ }

+

+ read\_lock(&tasklist\_lock);

```

+ if (pid != -1) {
+   ret = __kill_pgrp_info(sig, info,
+     pid ? find_vpid(-pid) : task_pgrp(current));
+ } else {
+   int retval = 0, count = 0;
+   struct task_struct * p;

-   read_lock(&tasklist_lock);
+   for_each_process(p) {
+     if (p->pid > 1 && !same_thread_group(p, current)) {
+       int err = group_send_sig_info(sig, info, p);
@@ -1150,14 +1158,10 @@ static int kill_something_info(int sig, struct siginfo *info, int pid)
+       retval = err;
+     }
+   }
-   read_unlock(&tasklist_lock);
+   ret = count ? retval : -ESRCH;
- } else if (pid < 0) {
-   ret = kill_pgrp_info(sig, info, find_vpid(-pid));
- } else {
-   ret = kill_pid_info(sig, info, find_vpid(pid));
- }
- rcu_read_unlock();
+ read_unlock(&tasklist_lock);
+
+   return ret;
+ }

```

--

1.5.3.4

---