
Subject: Re: + remove-the-likelypid-check-in-copy_process.patch added to -mm tree

Posted by [Oleg Nesterov](#) on Fri, 16 Mar 2007 17:02:55 GMT

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

Sukadev Bhattiprolu wrote:

```
> @@ -1237,26 +1237,24 @@ static struct task_struct *copy_process(
> }
> }
>
> - if (likely(p->pid)) {
> - add_parent(p);
> - tracehook_init_task(p);
> -
> - if (thread_group_leader(p)) {
> - pid_t pgid = process_group(current);
> - pid_t sid = process_session(current);
> -
> - p->signal->tty = current->signal->tty;
> - p->signal->pgrp = pgid;
> - set_signal_session(p->signal, process_session(current));
> - attach_pid(p, PIDTYPE_PGID, find_pid(pgid));
> - attach_pid(p, PIDTYPE_SID, find_pid(sid));
> + add_parent(p);
```

This means that idle threads (except "swapper") are visible to `for_each_process()` and `do_each_thread()`. Looks dangerous and somewhat strange to me.

Could you explain this change?

Oleg.

Containers mailing list

Containers@lists.osdl.org

<https://lists.osdl.org/mailman/listinfo/containers>
