Subject: Re: [PATCH] cgroup: fix a race condition in manipulating tsk->cg_list
Posted by akpm on Thu, 17 Apr 2008 05:16:02 GMT

On Thu, 17 Apr 2008 13:10:33 +0800 Li Zefan <lizf@cn.fujitsu.com> wrote:

> Andrew Morton wrote:
> > On Wed, 16 Apr 2008 21:17:34 -0700 "Paul Menage" <menage@google.com> wrote:
> >
> >> On Wed, Apr 16, 2008 at 9:11 PM, Andrew Morton
> >> <akpm@linux-foundation.org> wrote:
> >>> I don't fully understand the race. Both paths hold css_set_lock.
> >>>
> >>> Can you describe it in more detail please?
> >> Task A starts exiting, passes the check for unlinking current->cg_list.
> >
> > So cgroup_exit() sees !list_empty(tsk->cg_list)
> >
>
> cgroup_exit() sees list_empty(tsk->cg_list), then cgroup_enable_task_cg_list()
> links the task to the list, and then the task exited, so the list entry won't
> get deleted.

OK.

_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers