

---

Subject: Re: [PATCH] namespaces: fix race at task exit  
Posted by [Cedric Le Goater](#) on Thu, 25 Jan 2007 15:20:23 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Serge E. Hallyn wrote:

> In do\_exit(), the exit\_task\_namespaces() was placed after  
> exit\_notify() because exit\_notify ends up using the pid  
> namespace both to access the reaper, and for detaching the  
> pid. However, this placement allows an nfs server to reap  
> the task before exit\_task\_namespaces() completes.  
>  
> This patch moves the exit\_task\_namespaces() into release\_task,  
> below release\_thread() which puts the pids(), and just above  
> the call\_rcu(delayed\_put\_task\_struct). I believe this should  
> solve both problems.  
>  
> Signed-off-by: Serge E. Hallyn <serue@us.ibm.com>

I've run some tests on x86 and x86\_64: mounted a NFS share after  
having unshare(CLONE\_NEWNS) and I didn't reproduce the bug Daniel  
had found.

it looks safe.

C.

---

Containers mailing list  
Containers@lists.osdl.org  
<https://lists.osdl.org/mailman/listinfo/containers>

---