
Subject: Re: [RFC,PATCH] fix /sbin/init signal handling
Posted by [Oleg Nesterov](#) on Tue, 21 Aug 2007 17:04:43 GMT
[View Forum Message](#) <> [Reply to Message](#)

On 08/21, Serge E. Hallyn wrote:

```
>
> Quoting Oleg Nesterov (oleg@tv-sign.ru):
> > @@ -1841,14 +1865,6 @@ relock:
> >     if (sig_kernel_ignore(signr)) /* Default is nothing. */
> >         continue;
> >
> >
> > - /*
> > -  * Init of a pid space gets no signals it doesn't want from
> > -  * within that pid space. It can of course get signals from
> > -  * its parent pid space.
> > -  */
> > - if (current == child_reaper(current))
> > -     continue;
> > -
>
> Ok, so the idea is that this will now be caught when the signal is sent,
> using sig_ignored(), (i.e at send_sigqueue, send_group_sigqueue,
> specific_send_sig_info, and __group_send_sig_info) and so doesn't need
> to be checked here?
```

Yes.

```
> I was hoping that meant that sig_init_ignore() would always be called
> with current as the sending process, but I guess that's not the case?
```

Usually `current == sender`, but if the signal was sent from interrupt context, `current` is some random process.

```
> At least in get_signal_to_deliver() we might resend a signal, though
> I guess we assume the signal comes from current->parent, so maybe we
> can pass that as an argument...
```

`get_signal_to_deliver()` might resend a signal, but only when `current` is ptraced. In that case the signal will be delivered even if we are init, no problem. (except that ptracing of sub-namespace init is problem by itself).

Thanks for looking at this!

Oleg.

Containers mailing list

