Subject: Re: [PATCH 0/4] Fix race between sk_filter reassign and sk_clone()
Posted by davem on Fri, 19 Oct 2007 07:52:45 GMT
View Forum Message <> Reply to Message

From: Pavel Emelyanov <xemul@openvz.org>
Date: Fri, 19 Oct 2007 11:37:02 +0400

> David Miller wrote:
> > From: Olof Johansson <olof@lixom.net>
> > Date: Thu, 18 Oct 2007 21:29:47 -0500
> >
> >> So, looks like rcu_dereference() returned NULL. I don't know the
> >> filter code at all, but it seems like it might be a valid case?
> >> sk_detach_filter() seems to handle a NULL sk_filter, at least.
> >>
> >>
> >> So, this needs review by someone who knows the filter, but it fixes the
> >> problem for me:
>
> Yes. The NULL filter is a valid case, when there are no
> filters attached at all. So this fix is correct.
>
> Thanks, Olof. Sorry, Dave :(

No worries, thanks for reviewing.