Subject: Re: [PATCH 0/4] Fix race between sk_filter reassign and sk_clone()
Posted by Pavel Emelianov on Fri, 19 Oct 2007 07:37:02 GMT
View Forum Message <> Reply to Message

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 :(

>>
>> Signed-off-by: Olof Johansson <olof@lixom.net>

Acked-by: Pavel Emelyanov <xemul@openvz.org>

> I've applied this for now to my net-2.6 tree, thanks Olof
> for tracking this down.
>
> Pavel please take a look at this and let me know if it should
> fixed in some other way.
>
> Thanks!
>