Subject: Re: [PATCH 2/3] Lost locking in fl6_sock_lookup
Posted by Pavel Emelianov on Thu, 18 Oct 2007 12:22:49 GMT
View Forum Message <> Reply to Message

David Miller wrote:
> From: Pavel Emelyanov <xemul@openvz.org>
> Date: Thu, 18 Oct 2007 15:53:52 +0400
>
>> This routine scans the ipv6_fl_list whose update is
>> protected with the socket lock and the ip6_sk_fl_lock.
>>
>> Since the socket lock is not taken in the lookup, use
>> the other one.
>>
>> Signed-off-by: Pavel Emelyanov <xemul@openvz.org>
>
> Applied.
>
> But I notice that I was wrong in my email, we don't
> hold the socket lock here.
>
> What prevents an unlink from the socket's list
> and thus a reference count of zero occurring for
> a brief moment?

Oops. You're right here :(I looked at the ip6_fl_lock
and messed it with the ip6_sk_fl_lock.

Should I resend the whole patch, or just make an
incremental one?

Thanks,
Pavel