Subject: Re: [PATCH 2/3] Lost locking in fl6_sock_lookup
Posted by davem on Thu, 18 Oct 2007 12:16:47 GMT
View Forum Message <> Reply to Message

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?