Subject: Re: [NETLINK] Don't attach callback to a going-away netlink socket
Posted by Evgeniy Polyakov on Wed, 18 Apr 2007 08:44:16 GMT

View Forum Message <> Reply to Message

On Wed, Apr 18, 2007 at 12:32:40PM +0400, Pavel Emelianov (xemul@sw.ru) wrote:
> Evgeniy Polyakov wrote:
> > On Wed, Apr 18, 2007 at 12:16:18PM +0400, Pavel Emelianov (xemul@sw.ru) wrote:
> >> Sorry, I forgot to put netdev and David in Cc when I first sent it.
> >>
> >> There is a race between netlink_dump_start() and netlink_release()
> >> that can lead to the situation when a netlink socket with non-zero
> >> callback is freed.
> >
> > Out of curiosity, why not to fix a netlink_dump_start() to remove
> > callback in error path, since in 'no-error' path it removes it in
>
> Error path is not relevant here. The problem is that we
> keep a calback on a socket that is about to be freed.

Yes, you are right, that it will not be freed in netlink_release(),
but it will be freed in netlink_dump() after it is processed (in no-error
path only though).

--
 Evgeniy Polyakov