Subject: Re: [PATCH] Don't attach callback to a going-away netlink socket
Posted by Patrick McHardy on Mon, 16 Apr 2007 12:55:08 GMT
View Forum Message <> Reply to Message

Pavel Emelianov wrote:
> Patrick McHardy wrote:
>
>>>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.
>>
>>
>>Can you describe the race in more detail please?
>>
>
> Here it is:
>
> [...]
> The proposal it to make sock_orphan before detaching the callback
> in netlink_release() and to check for the sock to be SOCK_DEAD in
> netlink_dump_start() before setting a new callback.

Thanks, good catch. Your patch also looks good.

Acked-by: Patrick McHardy <kaber@trash.net>