Subject: Re: [PATCH] OOPS with NETLINK_FIB_LOOKUP netlink socket
Posted by den on Fri, 21 Dec 2007 09:37:46 GMT
View Forum Message <> Reply to Message

David Miller wrote:
> From: "Denis V. Lunev" <den@openvz.org>
> Date: Fri, 21 Dec 2007 12:00:43 +0300
>
>> nl_fib_input re-reuses incoming skb to send the reply. This means that this
>> packet will be freed twice, namely in:
>> - netlink_unicast_kernel
>> - on receive path
>> Use clone to send as a cure, the caller is responsible for kfree_skb on error.
>>
>> Thanks to Alexey Dobryan, who originally found the problem.
>>
>> Signed-off-by: Denis V. Lunev <den@openvz.org>
>
> What introduced this bug? This code didn't have this
> problem previously.
>

commit cd40b7d3983c708aabe3d3008ec64ffce56d33b0
Author: Denis V. Lunev <den@openvz.org>
Date: Wed Oct 10 21:15:29 2007 -0700