Subject: Re: [PATCH] OOPS with NETLINK_FIB_LOOKUP netlink socket
Posted by davem on Fri, 21 Dec 2007 09:33:21 GMT
View Forum Message <> Reply to Message

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.