Subject: Re: [PATCH] bridge: Reset IPCB on forward non-local packets in br_handle_frame_finish()

Posted by davem on Wed, 02 Nov 2011 20:09:05 GMT

View Forum Message <> Reply to Message

From: Vasily Averin <vvs@parallels.com>
Date: Wed, 02 Nov 2011 23:08:57 +0400

> if dst is not local br_handle_frame_finish() does not clone original skb and
> forgets to reset IPCB before return to IP stack. it can lead to stack corruption
> in icmp_send()
>
> Signed-off-by: Vasily Averin <vvs@sw.ru>

Nothing is worse than posting a patch that doesn't even compile.

And I really mean _nothing_.