Subject: Re: [PATCH] bridge: Reset IPCB on forward non-local packets in br_handle_frame_finish()
Posted by Vasily Averin on Wed, 02 Nov 2011 20:03:53 GMT
View Forum Message <> Reply to Message

On 11/02/2011 11:31 PM, Stephen Hemminger wrote:
> On Wed, 02 Nov 2011 23:08:57 +0400
> Vasily Averin <vvs@parallels.com> wrote:
>
>> 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()

> What kernel version are you using? There were several previous fixes
> in br_netfilter to deal with this type of issue over the last year.

Originally it was noticed on RHEL6-based kernel

You are right, in mainline this issue was fixed in br_nf_forward_ip() long time ago.

thank you,
 Vasily Averin