Subject: [PATCH] bridge: Reset IPCB on forward non-local packets in br_handle_frame_finish()
Posted by Vasily Averin on Wed, 02 Nov 2011 19:08:57 GMT
View Forum Message <> Reply to Message

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>
---
 net/bridge/br_input.c | 5 +++--
 1 files changed, 3 insertions(+), 2 deletions(-)

```
diff --git a/net/bridge/br_input.c b/net/bridge/br_input.c
index f06ee39..6be8d00 100644
--- a/net/bridge/br_input.c
+++ b/net/bridge/br_input.c
@@ -93,10 +93,11 @@ int br_handle_frame_finish(struct sk_buff *skb)
     skb2 = skb;

   br->dev->stats.multicast++;
- } else if ((dst = __br_fdb_get(br, dest)) && dst->is_local) {
+ } else if ((dst = __br_fdb_get(br, dest)) != NULL) {
   skb2 = skb;
   /* Do not forward the packet since it's local. */
-  skb = NULL;
+  if (dst->is_local) {
+   skb = NULL;
  }

  if (skb) {
-- 1.7.5.4
```