author	Wei Yongjun <weiyongjun1@huawei.com>	2022-11-14 11:05:19 +0000
committer	Jakub Kicinski <kuba@kernel.org>	2022-11-15 20:22:19 -0800
commit	2929cceb2fcf0ded7182562e4888afafece82cce (patch)	
tree	f9bacf2fc24e734004408b7450a82eb7fdc600a7	
parent	c9b895c6878bdb6789dc1d7af60fd10f4a9f1937 (diff)	
download	linux-2929cceb2fcf0ded7182562e4888afafece82cce.tar.gz	

diff options

context: 3

space: include

mode: unified

net/x25: Fix skb leak in x25_lapb_receive_frame()

```
x25_lapb_receive_frame() using skb_copy() to get a private copy of
skb, the new skb should be freed in the undersized/fragmented skb
error handling path. Otherwise there is a memory leak.

Fixes: cb101ed2c3c7 ("x25: Handle undersized/fragmented skbs")
Signed-off-by: Wei Yongjun <weiyongjun1@huawei.com>
Acked-by: Martin Schiller <ms@dev.tdt.de>
Link: https://lore.kernel.org/r/20221114110519.514538-1-weiyongjun@huaweicloud.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
```

Diffstat

-rw-r--r-- net/x25/x25_dev.c 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/net/x25/x25_dev.c b/net/x25/x25_dev.c
index 5259ef8f5242f3..748d8630ab58b9 100644
--- a/net/x25/x25_dev.c
+++ b/net/x25/x25_dev.c
@@ -117,7 +117,7 @@ int x25_lapb_receive_frame(struct sk_buff *skb, struct net_device *dev,

        if (!pskb_may_pull(skb, 1)) {
                x25_neigh_put(nb);
-               return 0;
+               goto drop;
        }

        switch (skb->data[0]) {
```