



author Szymon Heidrich <szymon.heidrich@gmail.com> 2023-03-13 23:00:45 +0100
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-22 13:28:06 +0100
commit [9fabdd79051a9fe51388df099aff6e4b660fedd2](#) (patch)
tree [f81aba0affb284a84efe894acefe90bb906e99a4](#)
parent [b0c202a8dc63008205a5d546559736507a9aae66](#) (diff)
download [linux-9fabdd79051a9fe51388df099aff6e4b660fedd2.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

net: usb: smsc75xx: Limit packet length to skb->len

[Upstream commit d8b228318935044daffe3a5bc07ee71a1f1424b8d]

Packet length retrieved from skb data may be larger than the actual socket buffer length (up to 9026 bytes). In such case the cloned skb passed up the network stack will leak kernel memory contents.

Fixes: d0cad871703b ("smc75xx: SMC LAN75xx USB gigabit ethernet adapter driver")

Signed-off-by: Szymon Heidrich <szymon.heidrich@gmail.com>

Signed-off-by: David S. Miller <davem@davemloft.net>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- drivers/net/usb/smsc75xx.c 3
```

1 files changed, 2 insertions, 1 deletions

diff --git a/drivers/net/usb/smsc75xx.c b/drivers/net/usb/smsc75xx.c

index aa848be459ec7b..229ff92e41cd97 100644

--- a/drivers/net/usb/smsc75xx.c

+++ b/drivers/net/usb/smsc75xx.c

```
@@ -2210,7 +2210,8 @@ static int smsc75xx_rx_fixup(struct usbnet *dev, struct sk_buff *skb)
                                dev->net->stats.rx_frame_errors++;
        } else {
                /* MAX_SINGLE_PACKET_SIZE + 4(CRC) + 2(COE) + 4(Vlan) */
-               if (unlikely(size > (MAX_SINGLE_PACKET_SIZE + ETH_HLEN + 12))) {
+               if (unlikely(size > (MAX_SINGLE_PACKET_SIZE + ETH_HLEN + 12) ||
+                               size > skb->len)) {
                        netif_dbg(dev, rx_err, dev->net,
                                "size err rx_cmd_a=0x%08x\n",
                                rx_cmd_a);
```