| | | |
|---|---|---|
| author | Szymon Heidrich <szymon.heidrich@gmail.com> | 2023-03-13 23:00:45 +0100 |
| committer | Greg Kroah-Hartman <gregkh@linuxfoundation.org> | 2023-03-22 13:29:58 +0100 |
| commit | e294f0aa47e4844f3d3c8766c02accd5a76a7d4e (patch) | |
| tree | 36a25837186ed33c9a727377175c034a36685c45 | |
| parent | 9708efad9ba5095b9bb7916e11a135b3bd66c071 (diff) | |
| download | linux-e294f0aa47e4844f3d3c8766c02accd5a76a7d4e.tar.gz | |



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

```
[ Upstream commit d8b228318935044dafe3a5bc07ee71a1f1424b8d ]

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 ("smsc75xx: SMSC 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 378a12ae2d957c..0b3d11e28faa72 100644
--- a/drivers/net/usb/smsc75xx.c
+++ b/drivers/net/usb/smsc75xx.c
@@ -2211,7 +2211,8 @@ 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);
```