author	Szymon Heidrich <szymon.heidrich@gmail.com>	2023-03-13 23:00:45 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-22 13:33:47 +0100
commit	c7bdc137ca163b90917c1eeba4f1937684bd4f8b (patch)	
tree	81e33f2887729767e540d4dd6d77c031d41405e1	
parent	3517584cf1b35bd02f4a90267ddf9dcf17bd9c87 (diff)	
download	linux-c7bdc137ca163b90917c1eeba4f1937684bd4f8b.tar.gz	

diff options

context: 3
space: include
mode: unified

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 95de452ff4dad5..db34f8d1d6051f 100644
--- a/drivers/net/usb/smsc75xx.c
+++ b/drivers/net/usb/smsc75xx.c
@@ -2212,7 +2212,8 @@ 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);
```