author	Szymon Heidrich <szymon.heidrich@gmail.com>	2023-03-16 11:19:54 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-30 12:50:53 +0200
commit	70eb25c6a6cde149affe8a587371a3a8ad295ba0 (patch)	
tree	003f1c3ad7446b1498486a3bbbc699a40a492e5b	
parent	aa339328a3abca959bf4b8429617c436e980defe (diff)	
download	linux-70eb25c6a6cde149affe8a587371a3a8ad295ba0.tar.gz	

net: usb: smsc95xx: Limit packet length to skb->len

```
[ Upstream commit ff821092cf02a70c2bccd2d19269f01e29aa52cf ]

Packet length retrieved from descriptor may be larger than
the actual socket buffer length. In such case the cloned
skb passed up the network stack will leak kernel memory contents.

Fixes: 2f7ca802bdae ("net: Add SMSC LAN9500 USB2.0 10/100 ethernet adapter driver")
Signed-off-by: Szymon Heidrich <szymon.heidrich@gmail.com>
Reviewed-by: Jakub Kicinski <kuba@kernel.org>
Link: https://lore.kernel.org/r/20230316101954.75836-1-szymon.heidrich@gmail.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- drivers/net/usb/smsc95xx.c 6

1 files changed, 6 insertions, 0 deletions

```
diff --git a/drivers/net/usb/smsc95xx.c b/drivers/net/usb/smsc95xx.c
index 32d2c60d334dc7..563ecd27b93ea5 100644
--- a/drivers/net/usb/smsc95xx.c
+++ b/drivers/net/usb/smsc95xx.c
@@ -1833,6 +1833,12 @@ static int smsc95xx_rx_fixup(struct usbnet *dev, struct sk_buff *skb)
                size = (u16)((header & RX_STS_FL_) >> 16);
                align_count = (4 - ((size + NET_IP_ALIGN) % 4)) % 4;

+               if (unlikely(size > skb->len)) {
+                       netif_dbg(dev, rx_err, dev->net,
+                                 "size err header=0x%08x\n", header);
+                       return 0;
+               }
+
                if (unlikely(header & RX_STS_ES_)) {
                        netif_dbg(dev, rx_err, dev->net,
                                  "Error header=0x%08x\n", header);
```