[Slirp] [PATCH] slirp: check pkt_len before reading protocol header

P J P ppandit at redhat.com
Thu Nov 26 13:57:06 UTC 2020

- Next message (by thread): [Slirp] [PATCH] slirp: check pkt_len before reading protocol header
- **Messages sorted by:** [date] [thread] [subject] [author]

```
From: Prasad J Pandit <pjp at fedoraproject.org>

While processing ARP/NCSI packets in 'arp_input' or 'ncsi_input'
routines, ensure that pkt_len is large enough to accommodate the
respective protocol headers, lest it should do an OOB access.
Add check to avoid it.

Reported-by: Qiuhao Li <Qiuhao.Li at outlook.com>
Signed-off-by: Prasad J Pandit <pjp at fedoraproject.org>
---
 src/ncsi.c  | 4 ++++
 src/slirp.c | 4 ++++
 2 files changed, 8 insertions(+)

diff --git a/src/ncsi.c b/src/ncsi.c
index 3c1dfef..75dcc08 100644
--- a/src/ncsi.c
+++ b/src/ncsi.c
@@ -148,6 +148,10 @@ void ncsi_input(Slirp *slirp, const uint8_t *pkt, int pkt_len)
     uint32_t checksum;
     uint32_t *pchecksum;

+    if (pkt_len < ETH_HLEN + sizeof(struct ncsi_pkt_hdr)) {
+        return; /* packet too short */
+    }
+
     memset(ncsi_reply, 0, sizeof(ncsi_reply));

     memset(reh->h_dest, 0xff, ETH_ALEN);
diff --git a/src/slirp.c b/src/slirp.c
index 9bead0c..abb6f9a 100644
--- a/src/slirp.c
+++ b/src/slirp.c
@@ -860,6 +860,10 @@ static void arp_input(Slirp *slirp, const uint8_t *pkt, int pkt_len)
         return;
     }

+    if (pkt_len < ETH_HLEN + sizeof(struct slirp_arphdr)) {
+        return; /* packet too short */
+    }
+
     ar_op = ntohs(ah->ar_op);
     switch (ar_op) {
     case ARPOP_REQUEST:
--
2.28.0
```

- Next message (by thread): [Slirp] [PATCH] slirp: check pkt_len before reading protocol header
- **Messages sorted by:** [date] [thread] [subject] [author]
