

qemu-devel[\[Top\]](#)[\[All Lists\]](#)Search [Advanced](#)[\[Date Prev\]](#)[\[Date Next\]](#)[\[Thread Prev\]](#)[\[Thread Next\]](#)[\[Date Index\]](#)[\[Thread Index\]](#)

[Qemu-devel] [PULL 22/25] rtl8139: fix possible out of bound access

From: Jason Wang**Subject:** [Qemu-devel] [PULL 22/25] rtl8139: fix possible out of bound access**Date:** Wed, 26 Sep 2018 11:16:47 +0800

In rtl8139_do_receive(), we try to assign size_ to size which converts from size_t to integer. This will cause troubles when size_ is greater INT_MAX, this will lead a negative value in size and it can then pass the check of size < MIN_BUF_SIZE which may lead out of bound access of for both buf and buf1.

Fixing by converting the type of size to size_t.

CC: address@hidden

Reported-by: Daniel Shapira <address@hidden>

Reviewed-by: Michael S. Tsirkin <address@hidden>

Signed-off-by: Jason Wang <address@hidden>

hw/net/rtl8139.c | 8 ++++----

1 file changed, 4 insertions(+), 4 deletions(-)

diff --git a/hw/net/rtl8139.c b/hw/net/rtl8139.c

index 46daa16202..2342a095e3 100644

--- a/hw/net/rtl8139.c

+++ b/hw/net/rtl8139.c

@@ -817,7 +817,7 @@ static ssize_t rtl8139_do_receive(NetClientState *nc, const uint8_t *buf, size_t

RTL8139State *s = qemu_get_nic_opaque(nc);

PCIDevice *d = PCI_DEVICE(s);

/* size is the length of the buffer passed to the driver */

- int size = size_;

+ size_t size = size_;

const uint8_t *dot1q_buf = NULL;

uint32_t packet_header = 0;

@@ -826,7 +826,7 @@ static ssize_t rtl8139_do_receive(NetClientState *nc, const uint8_t *buf, size_t

static const uint8_t broadcast_macaddr[6] =

{ 0xff, 0xff, 0xff, 0xff, 0xff, 0xff };

- DPRINTF(">>> received len=%d\n", size);

+ DPRINTF(">>> received len=%zu\n", size);

/* test if board clock is stopped */

if (!s->clock_enabled)

@@ -1035,7 +1035,7 @@ static ssize_t rtl8139_do_receive(NetClientState *nc, const uint8_t *buf, size_t

if (size+4 > rx_space)

{

- DPRINTF("C+ Rx mode : descriptor %d size %d received %d + 4\n",

```

+         DPRINTF("C+ Rx mode : descriptor %d size %d received %zu + 4\n",
+                 descriptor, rx_space, size);

        s->IntrStatus |= RxOverflow;
@@ -1148,7 +1148,7 @@ static ssize_t rtl8139_do_receive(NetClientState *nc,
const uint8_t *buf, size_t
    if (avail != 0 && RX_ALIGN(size + 8) >= avail)
    {
-         DPRINTF("rx overflow: rx buffer length %d head 0x%04x "
+         "read 0x%04x == available 0x%04x need 0x%04x\n",
+         "read 0x%04x == available 0x%04x need 0x%04zx\n",
        s->RxBufferSize, s->RxBufAddr, s->RxBufPtr, avail, size + 8);

        s->IntrStatus |= RxOverflow;
--
2.17.1

```

reply via email to

Jason Wang

[\[Prev in Thread\]](#)

Current Thread

[\[Next in Thread\]](#)

- [\[Qemu-devel\] \[PULL 00/25\] Net patches](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 25/25\] e1000: indicate dropped packets in HW counters](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 24/25\] net: ignore packet size greater than INT_MAX](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 23/25\] pcnet: fix possible buffer overflow](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 22/25\] rtl8139: fix possible out of bound access](#), Jason Wang <=
 - [\[Qemu-devel\] \[PULL 19/25\] docs: Add COLO status diagram to COLO-FT.txt](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 20/25\] clean up callback when del virtqueue](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 14/25\] COLO: flush host dirty ram from cache](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 21/25\] ne2000: fix possible out of bound access in ne2000 receive](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 17/25\] COLO: notify net filters about checkpoint/failover event](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 18/25\] COLO: quick failover process by kick COLO thread](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 13/25\] savevm: split the process of different stages for loadvm/savevm](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 15/25\] filter: Add handle_event method for NetFilterClass](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 11/25\] qapi/migration.json: Rename COLO unknown mode to none mode.](#), Jason Wang, 2018/09/25
 - [\[Qemu-devel\] \[PULL 05/25\] COLO: Add block replication into colo process](#), Jason Wang, 2018/09/25

-
- Prev by Date: [\[Qemu-devel\] \[PULL 23/25\] pcnet: fix possible buffer overflow](#)
 - Next by Date: [\[Qemu-devel\] \[PULL 19/25\] docs: Add COLO status diagram to COLO-FT.txt](#)
 - Previous by thread: [\[Qemu-devel\] \[PULL 23/25\] pcnet: fix possible buffer overflow](#)
 - Next by thread: [\[Qemu-devel\] \[PULL 19/25\] docs: Add COLO status diagram to COLO-FT.txt](#)
 - Index(es):

5/1/26, 7:41 PM

[Qemu-devel] [PULL 22/25] rt18139: fix possible out of bound access

- [Date](#)
- [Thread](#)