QEMU: net: vmxnet: integer overflow may crash guest

Bug #1913873 reported by P J P on 2021-01-30

This bug affects 2 people 266

Affects	Status	Importance	Assigned to	Milestone
QEMU	Expired	Undecided	Unassigned	

Bug Description

```
* Gaoning Pan from Zhejiang University & Ant Security Light-Year Lab
reported a malloc failure
  issue locates in vmxnet3_activate_device() of qemu/hw/net/vmxnet3.c NIC
emulator

* This issue is reproducible because while activating the NIC device,
vmxnet3_activate_device
  does not validate guest supplied configuration values against predefined
min/max limits.

@@ -1420,6 +1420,7 @@ static void vmxnet3_activate_device(VMXNET3State *s)
     vmxnet3_setup_rx_filtering(s);
     /* Cache fields from shared memory */
     s->mtu = VMXNET3_READ_DRV_SHARED32(d, s->drv_shmem,
devRead.misc.mtu);
+ assert(VMXNET3_MIN_MTU <= s->mtu && s->mtu < VMXNET3_MAX_MTU); <= Did
not check if MTU is within range
     VMW_CFPRN("MTU is %u", s->mtu);

     s->max_rx_frags =
@@ -1473,6 +1474,9 @@ static void vmxnet3_activate_device(VMXNET3State *s)
         /* Read rings memory locations for TX queues */
         pa = VMXNET3_READ_TX_QUEUE_DESCR64(d, qdescr_pa,
conf.txRingBasePA);
         size = VMXNET3_READ_TX_QUEUE_DESCR32(d, qdescr_pa,
conf.txRingSize);
+ if (size > VMXNET3_TX_RING_MAX_SIZE) { <= Did not check TX ring size
+ size = VMXNET3_TX_RING_MAX_SIZE;
+ }

         vmxnet3_ring_init(d, &s->txq_descr[i].tx_ring, pa, size,
                           sizeof(struct Vmxnet3_TxDesc), false);
@@ -1483,6 +1487,9 @@ static void vmxnet3_activate_device(VMXNET3State *s)
         /* TXC ring */
         pa = VMXNET3_READ_TX_QUEUE_DESCR64(d, qdescr_pa, conf.compRingBa
sePA);
         size = VMXNET3_READ_TX_QUEUE_DESCR32(d, qdescr_pa,
conf.compRingSize);
+ if (size > VMXNET3_TC_RING_MAX_SIZE) { <= Did not check TC ring size
+ size = VMXNET3_TC_RING_MAX_SIZE;
+ }
         vmxnet3_ring_init(d, &s->txq_descr[i].comp_ring, pa, size,
                           sizeof(struct Vmxnet3_TxCompDesc), true);
         VMXNET3_RING_DUMP(VMW_CFPRN, "TXC", i, &s->txq_descr[i]
.comp_ring);
@@ -1524,6 +1531,9 @@ static void vmxnet3_activate_device(VMXNET3State *s)
             /* RX rings */
             pa = VMXNET3_READ_RX_QUEUE_DESCR64(d, qd_pa, conf.rxRingBase
PA[j]);
             size = VMXNET3_READ_RX_QUEUE_DESCR32(d, qd_pa,
conf.rxRingSize[j]);
+ if (size > VMXNET3_RX_RING_MAX_SIZE) { <= Did not check RX ring size
+ size = VMXNET3_RX_RING_MAX_SIZE;
+ }
             vmxnet3_ring_init(d, &s->rxq_descr[i].rx_ring[j], pa, size,
                               sizeof(struct Vmxnet3_RxDesc), false);
             VMW_CFPRN("RX queue %d:%d: Base: %" PRIx64 ", Size: %d",
@@ -1533,6 +1543,9 @@ static void vmxnet3_activate_device(VMXNET3State *s)
         /* RXC ring */
         pa = VMXNET3_READ_RX_QUEUE_DESCR64(d, qd_pa, conf.compRingBa
sePA);
         size = VMXNET3_READ_RX_QUEUE_DESCR32(d, qd_pa,
conf.compRingSize);
+ if (size > VMXNET3_RC_RING_MAX_SIZE) { <= Did not check RC ring size
+ size = VMXNET3_RC_RING_MAX_SIZE;
+ }

This may lead to potential integer overflow OR OOB buffer access issues.
```

Tags: cve security

CVE References

2021-20203

P J P (pjps) wrote on 2021-01-30: #1

```
CVE-2021-20203 assigned by Red Hat Inc.
```

P J P (pjps) on 2021-01-30

```
information type:Private Security → Public Security
```

Alexander Bulekov (a1xndr) wrote on 2021-01-31: #2

```
Is this the same as https://bugs.launchpad.net/qemu/+bug/1890152 ?
```

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

Duplicates of this bug

Bug #1890152

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Jason Wang
P J P

May be notified

Alexander Bulekov
Alexander Nevench...
Anthony Liguori
Chun-Hung Chen
Daniel Tai
Haochen Zhang
Julio Faracco
Liang Yan
Michael Rowland H...
QiangGuan
Richard Zhang
Spencer Yu
Thomas Bergmann
ZhiQiang Yan
chen
copacule
grphilar
guangming liu
hotdigi
liaoxiaojun
longxingmiao
qemu-devel-ml
superleaf1995
vrozenfe
wangzhh
wlfightup

Remote bug watches

auto-gitlab.com-qemu-project-qemu-- #308 [closed Launchpad Security]

Bug watches keep track of this bug in other bug trackers.

P J P (pjps) wrote on 2021-01-31: #3

```
Yes, from the trace looks same.
```

Thomas Huth (th-huth) wrote on 2021-05-14: **Moved bug report** #4

```
This is an automated cleanup. This bug report has been moved to QEMU's
new bug tracker on gitlab.com and thus gets marked as 'expired' now.
Please continue with the discussion here:

 https://gitlab.com/qemu-project/qemu/-/issues/308

Changed in qemu:
status:New → Expired
```

See full activity log

To post a comment you must log in.