Closed Issue created 3 months ago by Siqi Chen

tulip: DMA reentrancy issue leads to stack overflow (CVE-2022-2962)

Description of problem

A DMA reentrancy issue was found in the tulip emulation. When tulip reads or writes to rx/tx descriptor (tulip_desc_read/write) or copies rx/tx frame(tulip_copy_rx_bytes / tulip_copy_tx_buffers), it doesn't check whether the destination address is its own MMIO address. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition or, potentially, executing arbitrary code within the context of the QEMU process on the host.

Reproducer

```
cat << EOF | ./qemu-system-x86_64 -machine type=q35,accel=qtest \
-nodefaults -device tulip -qtest stdio \

outl 0xcf8 0x80000804             /* PCICMD—PCI Command Register */
outl 0xcfc 0x107                  /* Enables accesses */
outl 0xcf8 0x80000814             /* Memory Bar 1 */
outl 0xcfc 0xfebf1000             /* Set MMIO Address to 0xfebf1000 */
writel 0xfebf1000 0               /* tulip_reset */
writel 0xfebf1030 0x2001          /* set csr6 flags=CSR6_ST|CSR6_SR */
writel 0xfebf1020 0xfebf1008      /* set current_tx_desc to its MMIO address,and trigger tulip_desc_
EOF
```

Trace events

```
[I 1655571308.706424] OPENED
outl 0xcf8 0x80000804
[R +7.839894] outl 0xcf8 0x80000804
OK
[S +7.839916] OK
outl 0xcfc 0x107
[R +10.885790] outl 0xcfc 0x107
OK
[S +10.885947] OK
outl 0xcf8 0x80000814
[R +14.951836] outl 0xcf8 0x80000814
OK
[S +14.951864] OK
outl 0xcfc 0xfebf1000
[R +17.905809] outl 0xcfc 0xfebf1000
OK
[S +17.905969] OK
writel 0xfebf1000 0
[R +21.069936] writel 0xfebf1000 0
OK
[S +21.069966] OK
writel 0xfebf1030 0x2001
[R +23.897858] writel 0xfebf1030 0x2001
OK
[S +23.897897] OK
writel 0xfebf1020 0xfebf1008
[R +26.867841] writel 0xfebf1020 0xfebf1008
Segmentation fault (core dumped)
```

Stack trace

From gdb:

```
#0  0x000055cb2de15dba in address_space_read_full (as=0x55cb3041ee50, addr=4273934344, attrs=..., bu
#1  0x000055cb2de15f65 in address_space_rw (as=as@entry=0x55cb3041ee50, addr=<optimized out>, attrs=
```

```
#2  0x000055cb2dc9e074 in dma_memory_rw_relaxed (attrs=..., dir=DMA_DIRECTION_TO_DEVICE, len=4, buf=
#3  dma_memory_rw (attrs=..., dir=DMA_DIRECTION_TO_DEVICE, len=4, buf=0x7ffc7953d0a0, addr=427393434
#4  dma_memory_read (attrs=..., len=4, buf=0x7ffc7953d0a0, addr=4273934344, as=0x55cb3041ee50) at /h
#5  ldl_le_dma (attrs=..., pval=0x7ffc7953d0a0, addr=4273934344, as=0x55cb3041ee50) at /home/coc/Des
#6  ldl_le_pci_dma (attrs=..., val=0x7ffc7953d0a0, addr=4273934344, dev=0x55cb3041ec20) at /home/coc
#7  tulip_desc_read (s=s@entry=0x55cb3041ec20, p=4273934344, desc=desc@entry=0x7ffc7953d0a0) at ../h
#8  0x000055cb2dc9e5fd in tulip_xmit_list_update (s=s@entry=0x55cb3041ec20) at ../hw/net/tulip.c:683
#9  0x000055cb2dc9ec00 in tulip_write (opaque=0x55cb3041ec20, addr=<optimized out>, data=<optimized
#10 0x000055cb2de0ba53 in memory_region_write_accessor (mr=mr@entry=0x55cb3041f730, addr=8, value=va
#11 0x000055cb2de07abe in access_with_adjusted_size (addr=addr@entry=8, value=value@entry=0x7ffc7953
#12 0x000055cb2de0b03c in memory_region_dispatch_write (mr=mr@entry=0x55cb3041f730, addr=8, data=<op
#13 0x000055cb2de1212f in flatview_write_continue (fv=fv@entry=0x55cb30518dc0, addr=addr@entry=42739
#14 0x000055cb2de122aa in flatview_write (fv=0x55cb30518dc0, addr=addr@entry=4273934344, attrs=attrs
#15 0x000055cb2de15ee8 in address_space_write (as=as@entry=0x55cb3041ee50, addr=4273934344, attrs=..
#16 0x000055cb2de15f5e in address_space_rw (as=as@entry=0x55cb3041ee50, addr=<optimized out>, attrs=
#17 0x000055cb2dc9dd70 in dma_memory_rw_relaxed (attrs=..., dir=DMA_DIRECTION_FROM_DEVICE, len=4, bu
#18 dma_memory_rw (attrs=..., dir=DMA_DIRECTION_FROM_DEVICE, len=4, buf=0x7ffc7953d434, addr=4273934
#19 dma_memory_write (attrs=..., len=4, buf=0x7ffc7953d434, addr=4273934344, as=0x55cb3041ee50) at /
#20 stl_le_dma (attrs=..., val=<optimized out>, addr=4273934344, as=0x55cb3041ee50) at /home/coc/Des
#21 stl_le_pci_dma (attrs=..., val=<optimized out>, addr=4273934344, dev=0x55cb3041ec20) at /home/co
#22 tulip_desc_write (s=s@entry=0x55cb3041ec20, p=4273934344, desc=desc@entry=0x7ffc7953d4b0) at ../
#23 0x000055cb2dc9e6b9 in tulip_xmit_list_update (s=s@entry=0x55cb3041ec20) at ../hw/net/tulip.c:706
#24 0x000055cb2dc9ec00 in tulip_write (opaque=0x55cb3041ec20, addr=<optimized out>, data=<optimized
#25 0x000055cb2de0ba53 in memory_region_write_accessor (mr=mr@entry=0x55cb3041f730, addr=8, value=va
#26 0x000055cb2de07abe in access_with_adjusted_size (addr=addr@entry=8, value=value@entry=0x7ffc7953
#27 0x000055cb2de0b03c in memory_region_dispatch_write (mr=mr@entry=0x55cb3041f730, addr=8, data=<op
#28 0x000055cb2de1212f in flatview_write_continue (fv=fv@entry=0x55cb30518dc0, addr=addr@entry=42739
#29 0x000055cb2de122aa in flatview_write (fv=0x55cb30518dc0, addr=addr@entry=4273934344, attrs=attrs
#30 0x000055cb2de15ee8 in address_space_write (as=as@entry=0x55cb3041ee50, addr=4273934344, attrs=..
#31 0x000055cb2de15f5e in address_space_rw (as=as@entry=0x55cb3041ee50, addr=<optimized out>, attrs=
#32 0x000055cb2dc9dd70 in dma_memory_rw_relaxed (attrs=..., dir=DMA_DIRECTION_FROM_DEVICE, len=4, bu
......
```

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Activity

Alexander Bulekov mentioned in issue #556 3 months ago

Mauro Matteo Cascella @mauromatteo.cascella · 3 months ago

RHBZ: https://bugzilla.redhat.com/show_bug.cgi?id=2120631.

Zheyu Ma @ZheyuMa · 3 months ago

I also found this bug a few days ago and proposed a possible patch: https://lore.kernel.org/qemu-devel/20220821122943.835058-1-zheyuma97@gmail.com/

Philippe Mathieu-Daudé added Networking Security labels 3 months ago

Thomas Huth mentioned in commit `thuth/qemu@9d856ed0` 2 months ago

Thomas Huth @thuth · 2 months ago Reporter

Zheyu Ma's patch has been merged here (thanks!): 36a894ae Thus closing this ticket now. Fix will be released with QEMU 7.2.

Thomas Huth closed 2 months ago

Thomas Huth assigned to @ZheyuMa 2 months ago

Please register or sign in to reply