Closed · Issue created 1 year ago by **Mauro Matteo Cascella**

Infinite loop in xhci_ring_chain_length() in hw/usb/hcd-xhci.c (CVE-2020-14394)

Host environment

- Operating system: Fedora 33
- OS/kernel version: 5.13.16-100.fc33.x86_64
- Architecture: x86
- QEMU flavor: qemu-system-x86_64
- QEMU version: 6.1.50 (v6.1.0-861-g22651bced7)
- QEMU command line:

```
./x86_64-softmmu/qemu-system-x86_64 -enable-kvm -m 4G -device nec-usb-xhci,id=xhci,slots=64 -device usb-tablet,bus=xhc
```

Emulated/Virtualized environment

- Operating system: Fedora 32
- OS/kernel version: 5.11.22-100.fc32.x86_64
- Architecture: x86

Description of problem

An infinite loop issue was found in the USB xHCI controller emulation of QEMU. Specifically, function `xhci_ring_chain_length()` in hw/usb/hcd-xhci.c may get stuck while fetching empty TRBs from guest memory, since the exit conditions of the loop depend on values that are fully controlled by guest. A privileged guest user may exploit this issue to hang the QEMU process on the host, resulting in a denial of service.

Steps to reproduce

Build and load `xhci.ko` from within the guest:

1. make
2. insmod xhci.ko

Makefile

usb-xhci.h

xhci.c

Additional information

This issue was reported by Gaoning Pan (Zhejiang University) and Xingwei Li (Ant Security Light-Year Lab).

RH bug: https://bugzilla.redhat.com/show_bug.cgi?id=1908004.

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

Philippe Mathieu-Daudé added USB label 1 year ago

Philippe Mathieu-Daudé added TestCase label 1 year ago

Philippe Mathieu-Daudé added Security label 1 year ago

Thomas Huth assigned to @thuth 4 months ago

Thomas Huth @thuth · 4 months ago — Reporter

Is this problem still reproducible with the latest version of QEMU? I had a try with the given reproducer, and for me, it does not hang the host QEMU anymore (version 7.1-rc0).

Looking at the history of this function, it also seems like there has been a fix for this here:

`05f43d44`

But we should maybe also check the return value of dma_memory_read() there to make sure to exit the loob in case the memory cannot be read anymore...

Thomas Huth @thuth · 4 months ago — Reporter

OK, I was finally able to get the reproducer running again after adjusting the value of the XHCI_MMIO_BASE macro in the source to 0xfebd0000 (according to the BAR value in the output of "lspci -vvv").

The problem can indeed be fixed by checking the return value of dma_memory_read(). I'll send a patch.

Thomas Huth added workflow In Progress scoped label 4 months ago

Thomas Huth @thuth · 4 months ago — Reporter

https://lore.kernel.org/qemu-devel/20220802134834.454749-1-thuth@redhat.com/

Thomas Huth mentioned in commit `thuth/qemu@0b076ef2` 4 months ago

Thomas Huth mentioned in commit `thuth/qemu@effaf5a2` 4 months ago

Thomas Huth closed via commit `effaf5a2` 4 months ago

Thomas Huth mentioned in commit `victortoso/qemu@73ca4adf` 3 months ago

Thomas Huth mentioned in commit `victortoso/qemu@60e2cb27` 3 months ago

Thomas Huth mentioned in commit `lulu6/gitlabqemutmp@84fc8464` 2 weeks ago

Please register or sign in to reply