Closed Issue created 1 year ago by Alexander Bulekov

Stack-overflow in ldl_le_dma through intel-hda (CVE-2021-3611)

This was originally reported at: https://bugs.launchpad.net/qemu/+bug/1907497

Hello,

Reproducer

```
cat << EOF | ./qemu-system-i386 -machine q35 -nodefaults  -device \
intel-hda,id=hda0 -device hda-output,bus=hda0.0  -device \
hda-micro,bus=hda0.0 -device hda-duplex,bus=hda0.0  -qtest stdio
outl 0xcf8 0x80000804
outw 0xcfc 0x06
write 0x0 0x1 0x12
write 0x2 0x1 0x2a
outl 0xcf8 0x80000811
outl 0xcfc 0x6a4400
write 0x6a44005a 0x1 0x01
write 0x6a44005c 0x1 0x02
write 0x6a442050 0x4 0x0000446a
write 0x6a44204a 0x1 0x01
write 0x6a44204c 0x1 0x02
write 0x6a44005c 0x1 0x02
write 0x6a442050 0x4 0x0000446a
write 0x6a44204a 0x1 0x01
write 0x6a44204c 0x1 0x02
EOF
```

Stack-Trace

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==206150==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc65c59f28 (pc 0x55d4e6942706 bp 0x7ffc65c5a770 sp 0x7ffc6
#0 0x55d4e6942706 in __asan_memcpy (system-i386+0x227d706)
#1 0x55d4e804b2e2 in flatview_do_translate ../softmmu/physmem.c:515:12
#2 0x55d4e805f536 in flatview_translate ../softmmu/physmem.c:565:15
#3 0x55d4e805f536 in flatview_read ../softmmu/physmem.c:2879:10
#4 0x55d4e805f536 in address_space_read_full ../softmmu/physmem.c:2893:18
#5 0x55d4e765be3d in dma_memory_rw_relaxed include/sysemu/dma.h:88:12
#6 0x55d4e765be3d in dma_memory_rw include/sysemu/dma.h:127:12
#7 0x55d4e765be3d in dma_memory_read include/sysemu/dma.h:145:12
#8 0x55d4e765be3d in ldl_le_dma include/sysemu/dma.h:260:1
#9 0x55d4e765be3d in ldl_le_pci_dma include/hw/pci/pci.h:859:1
#10 0x55d4e765be3d in intel_hda_corb_run ../hw/audio/intel-hda.c:338:16
....
#430 0x55d4e8067e26 in flatview_write_continue ../softmmu/physmem.c:2777:23
#431 0x55d4e805f995 in flatview_write ../softmmu/physmem.c:2817:14
#432 0x55d4e805f995 in address_space_write ../softmmu/physmem.c:2909:18
#433 0x55d4e7652280 in dma_memory_rw_relaxed include/sysemu/dma.h:88:12
#434 0x55d4e7652280 in dma_memory_rw include/sysemu/dma.h:127:12
#435 0x55d4e7652280 in dma_memory_write include/sysemu/dma.h:163:12
#436 0x55d4e7652280 in stl_le_dma include/sysemu/dma.h:260:1
#437 0x55d4e7652280 in stl_le_pci_dma include/hw/pci/pci.h:859:1
#438 0x55d4e7652280 in intel_hda_response ../hw/audio/intel-hda.c:370:5
#439 0x55d4e765bb71 in intel_hda_corb_run ../hw/audio/intel-hda.c:342:9
#440 0x55d4e7f01f75 in memory_region_write_accessor ../softmmu/memory.c:492:5
#441 0x55d4e7f01a9a in access_with_adjusted_size ../softmmu/memory.c:554:18
#442 0x55d4e7f0155f in memory_region_dispatch_write ../softmmu/memory.c
#443 0x55d4e8067e26 in flatview_write_continue ../softmmu/physmem.c:2777:23
#444 0x55d4e805f995 in flatview_write ../softmmu/physmem.c:2817:14
#445 0x55d4e805f995 in address_space_write ../softmmu/physmem.c:2909:18
#446 0x55d4e7652280 in dma_memory_rw_relaxed include/sysemu/dma.h:88:12
#447 0x55d4e7652280 in dma_memory_rw include/sysemu/dma.h:127:12
#448 0x55d4e7652280 in dma_memory_write include/sysemu/dma.h:163:12
#449 0x55d4e7652280 in stl_le_dma include/sysemu/dma.h:260:1
#450 0x55d4e7652280 in stl_le_pci_dma include/hw/pci/pci.h:859:1
#451 0x55d4e7652280 in intel_hda_response ../hw/audio/intel-hda.c:370:5
#452 0x55d4e765bb71 in intel_hda_corb_run ../hw/audio/intel-hda.c:342:9
#453 0x55d4e7f01f75 in memory_region_write_accessor ../softmmu/memory.c:492:5
#454 0x55d4e7f01a9a in access_with_adjusted_size ../softmmu/memory.c:554:18
#455 0x55d4e7f0155f in memory_region_dispatch_write ../softmmu/memory.c
#456 0x55d4e8067e26 in flatview_write_continue ../softmmu/physmem.c:2777:23
#457 0x55d4e805f995 in flatview_write ../softmmu/physmem.c:2817:14
#458 0x55d4e805f995 in address_space_write ../softmmu/physmem.c:2909:18
#459 0x55d4e7652280 in dma_memory_rw_relaxed include/sysemu/dma.h:88:12
#460 0x55d4e7652280 in dma_memory_rw include/sysemu/dma.h:127:12
#461 0x55d4e7652280 in dma_memory_write include/sysemu/dma.h:163:12
#462 0x55d4e7652280 in stl_le_dma include/sysemu/dma.h:260:1
#463 0x55d4e7652280 in stl_le_pci_dma include/hw/pci/pci.h:859:1
#464 0x55d4e7652280 in intel_hda_response ../hw/audio/intel-hda.c:370:5
#465 0x55d4e765bb71 in intel_hda_corb_run ../hw/audio/intel-hda.c:342:9

SUMMARY: AddressSanitizer: stack-overflow (system-i386+0x227d706) in __asan_memcpy
==206150==ABORTING
```

OSS-Fuzz Report: https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=28435

libqtest Reproducer: 1907497.c

Thank you

Edited 11 months ago by Philippe Mathieu-Daudé

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 added Audio Fuzzer labels 1 year ago

Alexander Bulekov @a1xndr · 1 year ago Author Reporter

Launchpad comment from Gianluca Gabruelli (crazy8yte) on Mon, 21 Jun 2021 05:57:11 -0000

```
I think this [0] commit actually fixes this bug, can someone please
confirm it?

[0]
https://github.com/qemu/qemu/commit/1bf8b88f144bee747e386c88d45d772e066bbb36
```

Launchpad comment from Thomas Huth (th-huth) on Mon, 21 Jun 2021 07:18:56 -0000

```
No, I can still reproduce this issue with current version from the git
repo (commit 8f521741e1280f0957ac1) ... when I compile QEMU with Clang
and --enable-sanitizers, the reproducer still crashes with "ERROR:
AddressSanitizer: stack-overflow"
```

Launchpad comment from Mauro Matteo Cascella (mauro-cascella) on Tue, 22 Jun 2021 15:57:38 -0000

```
Just FYI, this issue was assigned CVE-2021-3611 by Red Hat.
```

Launchpad comment from Gianluca Gabruelli (crazy8byte) on Wed, 30 Jun 2021 15:04:09 -0000

```
@Thomas, could you try by compiling qemu with a commit close to the
timeframe mentioned here [0]?

[0] https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=28435#c2
```

Launchpad comment from Thomas Huth (th-huth) on Wed, 30 Jun 2021 16:44:51 -0000

```
@Gianluca: The problem still reproduces with the current master branch
(commit 13d5f87cc3b94bfccc5), so the problem is definitely not fixed
yet. So no, I certainly won't waste my time trying it on older versions.
```

Philippe Mathieu-Daudé assigned to @philmd_rh 1 year ago

Philippe Mathieu-Daudé changed milestone to %6.2 1 year ago

Philippe Mathieu-Daudé mentioned in issue #556 1 year ago

Philippe Mathieu-Daudé changed milestone to %7.0 1 year ago

Philippe Mathieu-Daudé @philmd_rh · 11 months ago

Proposed fix: https://lore.kernel.org/qemu-devel/20211218160912.1591633-1-philmd@redhat.com/ @crazybyte

Edited by Philippe Mathieu-Daudé 11 months ago

Philippe Mathieu-Daudé added Security label 11 months ago

Philippe Mathieu-Daudé changed title from **Stack-overflow in ldl_le_dma through intel-hda** to **Stack-overflow in ldl_le_dma through intel-hda (CVE-2021-3611)** 11 months ago

Philippe Mathieu-Daudé assigned to @philmd 11 months ago

Philippe Mathieu-Daudé mentioned in commit `thuth/qemu@19a54527` 8 months ago

Philippe Mathieu-Daudé mentioned in commit `thuth/qemu@79fa9983` 8 months ago

Peter Maydell mentioned in commit `b7a3a705` 8 months ago

Philippe Mathieu-Daudé closed via commit `79fa9983` 8 months ago

Philippe Mathieu-Daudé mentioned in commit `victortoso/qemu@d64658cc` 8 months ago

Philippe Mathieu-Daudé mentioned in commit `victortoso/qemu@587ae474` 8 months ago

Please register or sign in to reply