Closed Issue created 1 month ago by Alexander Bulekov

erst: undefined-behavior in memcpy in write_erst_record

Hello,

Build with --enable-sanitizers

Reproducer

```
cat << EOF | ./qemu-system-i386 -display none -machine accel=qtest, -m \
512M -object memory-backend-ram,id=erstnvram,size=0x10000 -device \
acpi-erst,memdev=erstnvram -nodefaults -qtest stdio
outl 0xcf8 0x80001010
outl 0xcfc 0xe0000000
outl 0xcf8 0x80001014
outl 0xcfc 0xe0002000
outl 0xcf8 0x80001004
outw 0xcfc 0x02
write 0xe00021b1 0x1 0xff
write 0xe00021b2 0x1 0xff
write 0xe00021b3 0x1 0xff
write 0xe0002203 0x1 0x01
write 0xe0000008 0x2 0x9c01
write 0xe0000000 0x1 0x04
write 0xe0000000 0x1 0x05
EOF
```

Stack-Trace

```
==2058857==ERROR: AddressSanitizer: memcpy-param-overlap: memory ranges [0x7fdff2c02000,0x7fe0f2c01f00) and [0x7fdfd1c0019c, 0x7fe0d
    #0 0x55db1ec2de44 in __asan_memcpy (/home/alxndr/Development/qemu-demo/qemu/build-asan/qemu-system-i386+0x1fe4e44)
    #1 0x55db1ee38955 in write_erst_record /home/alxndr/Development/qemu-demo/qemu/build-asan/../hw/acpi/erst.c:718:9
    #2 0x55db1ee373e3 in erst_reg_write /home/alxndr/Development/qemu-demo/qemu/build-asan/../hw/acpi/erst.c:827:41
    #3 0x55db20238038 in memory_region_write_accessor /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/memory.c:492:5
    #4 0x55db20237943 in access_with_adjusted_size /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/memory.c:566:18
    #5 0x55db20236ca3 in memory_region_dispatch_write /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/memory.c
    #6 0x55db20283265 in flatview_write_continue /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/physmem.c:2820:23
    #7 0x55db2027a704 in flatview_write /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/physmem.c:2862:12
    #8 0x55db2027a704 in address_space_write /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/physmem.c:2958:18
    #9 0x55db20290e93 in qtest_process_command /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/qtest.c:653:9
    #10 0x55db2028d198 in qtest_process_inbuf /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/qtest.c:796:9
    #11 0x55db20928d94 in fd_chr_read /home/alxndr/Development/qemu-demo/qemu/build-asan/../chardev/char-fd.c:72:9
    #12 0x7fdff81c3a9e in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x53a9e)
    #13 0x55db20ba9de3 in glib_pollfds_poll /home/alxndr/Development/qemu-demo/qemu/build-asan/../util/main-loop.c:297:9
    #14 0x55db20ba9de3 in os_host_main_loop_wait /home/alxndr/Development/qemu-demo/qemu/build-asan/../util/main-loop.c:320:5
    #15 0x55db20ba9de3 in main_loop_wait /home/alxndr/Development/qemu-demo/qemu/build-asan/../util/main-loop.c:596:11
    #16 0x55db1f819156 in qemu_main_loop /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/runstate.c:734:9
    #17 0x55db1ec63235 in qemu_default_main /home/alxndr/Development/qemu-demo/qemu/build-asan/../softmmu/main.c:37:14
    #18 0x7fdff79e5209 in __libc_start_call_main csu/../sysdeps/nptl/libc_start_call_main.h:58:16
    #19 0x7fdff79e52bb in __libc_start_main csu/../csu/libc-start.c:389:3
    #20 0x55db1ebb1ca0 in _start (/home/alxndr/Development/qemu-demo/qemu/build-asan/qemu-system-i386+0x1f68ca0)
```

Thanks

Edited 1 month ago by Alexander Bulekov

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 changed the description 1 month ago ·

Philippe Mathieu-Daudé added Fuzzer label 1 month ago

Philippe Mathieu-Daudé added ACPI label 1 month ago

Stefan Hajnoczi mentioned in commit 99a9b6ed 1 month ago

Misha Tsirkin mentioned in commit mitsirkin/qemu@863c5f87 1 month ago

Misha Tsirkin mentioned in commit mitsirkin/qemu@77d0732b 1 month ago

Misha Tsirkin mentioned in commit mitsirkin/qemu@adec0c33 4 weeks ago

Misha Tsirkin mentioned in commit mitsirkin/qemu@0bc0cb63 4 weeks ago

MST mentioned in commit mstredhat/qemu@24c89a88 4 weeks ago

MST mentioned in commit mstredhat/qemu@b37bb947 3 weeks ago

MST mentioned in commit mstredhat/qemu@defb7098 3 weeks ago

Stefan Hajnoczi closed via commit defb7098 3 weeks ago

Please register or sign in to reply