QEMU: scsi: use-after-free in mptsas_process_scsi_io_request() of mptsas1068 emulator

Bug #1914236 reported by P J P on 2021-02-02

This bug affects 1 person 258

Affects	Status	Importance	Assigned to	Milestone
QEMU	Fix Released	Undecided	Unassigned	

Bug Description

```
* Cheolwoo Myung of Seoul National University reported a use-after-free
issue in the SCSI Megaraid
  emulator of the QEMU.

* It occurs while handling mptsas_process_scsi_io_request(), as it does
not
  check a list in s->pending.

* This was found in version 5.2.0 (master)

==31872==ERROR: AddressSanitizer: heap-use-after-free on address
0x60c000107568 at pc 0x564514950c7c bp 0x7fff524ef4b0 sp 0x7fff524ef4a0
WRITE of size 8 at 0x60c000107568 thread T0
#0 0x564514950c7b in mptsas_process_scsi_io_request ../hw/scsi/mptsas.
c:306
#1 0x564514950c7b in mptsas_fetch_request ../hw/scsi/mptsas.c:775
#2 0x564514950c7b in mptsas_fetch_requests ../hw/scsi/mptsas.c:790
#3 0x56451585c25d in aio_bh_poll ../util/async.c:164
#4 0x5645158d7e7d in aio_dispatch ../util/aio-posix.c:381
#5 0x56451585be2d in aio_ctx_dispatch ../util/async.c:306
#6 0x7f1cc8af4416 in g_main_context_dispatch
(/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c416)
#7 0x56451583f059 in glib_pollfds_poll ../util/main-loop.c:221
#8 0x56451583f059 in os_host_main_loop_wait ../util/main-loop.c:244
#9 0x56451583f059 in main_loop_wait ../util/main-loop.c:520
#10 0x56451536b181 in qemu_main_loop ../softmmu/vl.c:1537
#11 0x5645143ddd3d in main ../softmmu/main.c:50
#12 0x7f1cc2650b96 in __libc_start_main
(/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#13 0x5645143eece9 in _start
(/home/cwmyung/prj/hyfuzz/src/qemu-repro/build/qemu-system-i386+0x1d55ce9)

0x60c000107568 is located 104 bytes inside of 120-byte region
[0x60c000107500,0x60c000107578)
freed by thread T0 here:
#0 0x7f1cca9777a8 in __interceptor_free
(/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7a8)
#1 0x56451495008b in mptsas_process_scsi_io_request ../hw/scsi/mptsas.
c:358
#2 0x56451495008b in mptsas_fetch_request ../hw/scsi/mptsas.c:775
#3 0x56451495008b in mptsas_fetch_requests ../hw/scsi/mptsas.c:790
#4 0x7fff524ef8bf (<unknown module>)

previously allocated by thread T0 here:
#0 0x7f1cca977d28 in __interceptor_calloc
(/usr/lib/x86_64-linux-gnu/libasan.so.4+0xded28)
#1 0x7f1cc8af9b10 in g_malloc0
(/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51b10)
#2 0x7fff524ef8bf (<unknown module>)

SUMMARY: AddressSanitizer: heap-use-after-free ../hw/scsi/mptsas.c:306
in mptsas_process_scsi_io_request
Shadow bytes around the buggy address:
0x0c1880018e50: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c1880018e60: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
0x0c1880018e70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c1880018e80: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c1880018e90: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
=>0x0c1880018ea0: fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd fa
0x0c1880018eb0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c1880018ec0: 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa
0x0c1880018ed0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1880018ee0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1880018ef0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
==31872==ABORTING

To reproduce this issue, please run the QEMU with the following command
line.

# To enable ASan option, please set configuration with the following
command
$ ./configure --target-list=i386-softmmu --disable-werror --enable-
```

```
sanitizers
$ make

# To reproduce this issue, please run the QEMU process with the
following command line.
$ ./qemu-system-i386 -m 512 -drive
file=./hyfuzz.img,index=0,media=disk,format=raw -device
mptsas1068,id=scsi -device scsi-hd,drive=SysDisk -drive
id=SysDisk,if=none,file=./disk.img
```

Tags: cve security

CVE References

2021-3392

P J P (pjps) wrote on 2021-02-02: #1

```
CVE-2021-3392 assigned by Red Hat In.c
```

P J P (pjps) on 2021-02-02

information type:Private Security → Public Security

P J P (pjps) wrote on 2021-02-02: #2

```
Upstream patch
  -> https://lists.gnu.org/archive/html/qemu-devel/2021-02/msg00488.html
```

Mauro Matteo Cascella (mauro-cascella) wrote on 2021-04-20: #3

```
Upstream commit:
https://git.qemu.org/?p=qemu.git;a=commit;h=3791642c8d60029adf9b00bcb4e3
4d7d8a1aea4d

Changed in qemu:
status:New → Fix Committed
```

Thomas Huth (th-huth) on 2021-04-30

```
Changed in qemu:
status:Fix Committed → Fix Released
```

See full activity log

To post a comment you must log in.