Heap-overflow in flatview_read through sdhci_data_transfer

Bug #1892960 reported by Alexander Bulekov on 2020-08-26

This bug affects 1 person 6

Affects	Status	Importance	Assigned to	Milestone
QEMU	Fix Released	Undecided	Unassigned	

Bug Description

```
Hello,
Reproducer:
cat << EOF | ./qemu-system-i386 -nodefaults \
-device sdhci-pci,sd-spec-version=3 \
-device sd-card,drive=mydrive \
-drive if=sd,index=0,file=null-co://,format=raw,id=mydrive \
-nographic -qtest stdio -accel qtest
outl 0xcf8 0x80001010
outl 0xcfc 0xd7055dba
outl 0xcf8 0x80001003
outl 0xcfc 0x86b1d733
writeq 0xd7055d2b 0x84126e0ed7d7355e
writeq 0xd7055d23 0x13bd7d7346e0129
writeq 0xd7055d05 0x615bfb845e05c42c
write 0x0 0x1 0x39
write 0x5 0x1 0x06
write 0x6 0x1 0x35
write 0x7 0x1 0x01
write 0x1350600 0x1 0x39
writew 0xd7055d0e 0x846e
write 0x1350600 0x1 0x29
write 0x1350602 0x1 0x1a
write 0x1350608 0x1 0x39
clock_step
writeq 0xd7055d03 0x6d00000026000000
clock_step
EOF

The trace:

[R +0.077745] outl 0xcf8 0x80001010
OK
[S +0.077773] OK
[R +0.077792] outl 0xcfc 0xd7055dba
OK
[S +0.077813] OK
[R +0.077826] outl 0xcf8 0x80001003
OK
[S +0.077835] OK
[R +0.077846] outl 0xcfc 0x86b1d733
OK
[S +0.080186] OK
[R +0.080204] writeq 0xd7055d2b 0x84126e0ed7d7355e
752161@1598405049.572123:sdhci_access wr8: addr[0x002b] <- 0x0000005e (94)
752161@1598405049.572133:sdhci_access wr32: addr[0x002c] <- 0x0ed7d735
(249026357)
752161@1598405049.572142:sdhci_access wr16: addr[0x0030] <- 0x0000126e
(4718)
752161@1598405049.572150:sdhci_access wr8: addr[0x0032] <- 0x00000084
(132)
OK
[S +0.080255] OK
[R +0.080267] writeq 0xd7055d23 0x13bd7d7346e0129
752161@1598405049.572176:sdhci_error Non-sequential access to Buffer Data
Port registeris prohibited

752161@1598405049.572181:sdhci_access wr8: addr[0x0023] <- 0x00000029 (41)
752161@1598405049.572187:sdhci_access wr32: addr[0x0024] <- 0xd7346e01
(3610537473)
752161@1598405049.572193:sdhci_access wr16: addr[0x0028] <- 0x00003bd7
(15319)
752161@1598405049.572200:sdhci_access wr8: addr[0x002a] <- 0x00000001 (1)
OK
[S +0.080303] OK
[R +0.080316] writeq 0xd7055d05 0x615bfb845e05c42c
752161@1598405049.572226:sdhci_access wr8: addr[0x0005] <- 0x0000002c (44)
752161@1598405049.572233:sdhci_access wr16: addr[0x0006] <- 0x000005c4
(1476)
752161@1598405049.572240:sdhci_access wr32: addr[0x0008] <- 0x5bfb845e
(1543210078)
752161@1598405049.572247:sdhci_access wr8: addr[0x000c] <- 0x00000061 (97)
OK
[S +0.080350] OK
[R +0.080362] write 0x0 0x1 0x39
OK
[S +0.080606] OK
[R +0.080617] write 0x5 0x1 0x06
OK
[S +0.080629] OK
[R +0.080639] write 0x6 0x1 0x35
OK
[S +0.080648] OK
[R +0.080657] write 0x7 0x1 0x01
OK
[S +0.080665] OK
[R +0.080675] write 0x1350600 0x1 0x39
OK
[S +0.080863] OK
[R +0.080875] writew 0xd7055d0e 0x846e
752161@1598405049.572786:sdhci_send_command CMD132 ARG[0x5bfb845e]
752161@1598405049.572810:sdhci_error timeout waiting for command response
752161@1598405049.572822:sdhci_adma_loop addr=0x01350600, len=0, attr=0x39
```

```
752161@1598405049.572827:sdhci_adma link: admasysaddr=0x1350600
752161@1598405049.572833:sdhci_adma_loop addr=0x00000000, len=0, attr=0x39
752161@1598405049.572837:sdhci_adma link: admasysaddr=0x0
752161@1598405049.572842:sdhci_adma_loop addr=0x01350600, len=0, attr=0x39
752161@1598405049.572845:sdhci_adma link: admasysaddr=0x1350600
752161@1598405049.572851:sdhci_adma_loop addr=0x00000000, len=0, attr=0x39
752161@1598405049.572854:sdhci_adma link: admasysaddr=0x0
752161@1598405049.572859:sdhci_adma_loop addr=0x01350600, len=0, attr=0x39
752161@1598405049.572862:sdhci_adma link: admasysaddr=0x1350600
752161@1598405049.572875:sdhci_access wr16: addr[0x000e] <- 0x0000846e
(33902)
OK
[S +0.080979] OK
[R +0.080991] write 0x1350600 0x1 0x29
OK
[S +0.081001] OK
[R +0.081011] write 0x1350602 0x1 0x1a
OK
[S +0.081019] OK
[R +0.081029] write 0x1350608 0x1 0x39
OK
[S +0.081037] OK
[R +0.081045] clock_step
752161@1598405049.572962:sdhci_adma_loop addr=0x00000000, len=26,
attr=0x29
752161@1598405049.572972:sdhci_adma_loop addr=0x00000000, len=0, attr=0x39
752161@1598405049.572977:sdhci_adma link: admasysaddr=0x0
752161@1598405049.572981:sdhci_adma_loop addr=0x01350600, len=0, attr=0x39
752161@1598405049.572985:sdhci_adma link: admasysaddr=0x1350600
752161@1598405049.572989:sdhci_adma_loop addr=0x00000000, len=26,
attr=0x29
752161@1598405049.572997:sdhci_adma_loop addr=0x00000000, len=0, attr=0x39
752161@1598405049.573001:sdhci_adma link: admasysaddr=0x0
OK 100
[S +0.081112] OK 100
[R +0.081126] writeq 0xd7055d03 0x6d00000026000000
752161@1598405049.573038:sdhci_access wr8: addr[0x0003] <- 0x00000000 (0)
752161@1598405049.573045:sdhci_access wr32: addr[0x0004] <- 0x00260000
(2490368)
752161@1598405049.573051:sdhci_access wr16: addr[0x0008] <- 0x00000000 (0)
752161@1598405049.573057:sdhci_access wr8: addr[0x000a] <- 0x0000006d
(109)
OK
[S +0.081162] OK
[R +0.081171] clock_step
752161@1598405049.573085:sdhci_adma_loop addr=0x01350600, len=0, attr=0x39
752161@1598405049.573090:sdhci_adma link: admasysaddr=0x1350600
752161@1598405049.573096:sdhci_adma_loop addr=0x00000000, len=26,
attr=0x29
=================================================================
==752161==ERROR: AddressSanitizer: heap-buffer-overflow on address
0x61500001e500 at pc 0x5651bce1a940 bp 0x7fff16a81f50 sp 0x7fff16a81718
WRITE of size 786432 at 0x61500001e500 thread T0
    #0 0x5651bce1a93f in __asan_memcpy (/home/alxndr/Development/
qemu/general-fuzz/build/qemu-system-i386+0x2d2893f)
    #1 0x5651bf4197ce in flatview_read_continue /home/alxndr/Development/
qemu/general-fuzz/build/../exec.c:3246:13
    #2 0x5651bf41bff3 in flatview_read /home/alxndr/Development/
qemu/general-fuzz/build/../exec.c:3279:12
    #3 0x5651bf41bb48 in address_space_read_full /home/alxndr/Development/
qemu/general-fuzz/build/../exec.c:3292:18
    #4 0x5651bf41cce8 in address_space_rw /home/alxndr/Development/
qemu/general-fuzz/build/../exec.c:3320:16
    #5 0x5651bd623b67 in dma_memory_rw_relaxed /home/alxndr/Development/
qemu/general-fuzz/include/sysemu/dma.h:87:18
    #6 0x5651bd623585 in dma_memory_rw /home/alxndr/Development/
qemu/general-fuzz/include/sysemu/dma.h:110:12
    #7 0x5651bd6227b7 in dma_memory_read /home/alxndr/Development/
qemu/general-fuzz/include/sysemu/dma.h:116:12
    #8 0x5651bd61b052 in sdhci_do_adma /home/alxndr/Development/
qemu/general-fuzz/build/../hw/sd/sdhci.c:792:21
    #9 0x5651bd60d3c4 in sdhci_data_transfer /home/alxndr/Development/
qemu/general-fuzz/build/../hw/sd/sdhci.c:887:13
    #10 0x5651c0c4d917 in timerlist_run_timers /home/alxndr/Development/
qemu/general-fuzz/build/../util/qemu-timer.c:572:9
    #11 0x5651c0c4de51 in qemu_clock_run_timers /home/alxndr/Development/
qemu/general-fuzz/build/../util/qemu-timer.c:586:12
    #12 0x5651bf562a13 in qtest_clock_warp /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/cpus.c:507:9
    #13 0x5651bf74f5d8 in qtest_process_command /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/qtest.c:665:9
    #14 0x5651bf73d63e in qtest_process_inbuf /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/qtest.c:710:9
    #15 0x5651bf73c3e3 in qtest_read /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/qtest.c:722:5
    #16 0x5651c0842762 in qemu_chr_be_write_impl /home/alxndr/Development/
qemu/general-fuzz/build/../chardev/char.c:188:9
    #17 0x5651c08428aa in qemu_chr_be_write /home/alxndr/Development/
qemu/general-fuzz/build/../chardev/char.c:200:9
    #18 0x5651c0868514 in fd_chr_read /home/alxndr/Development/
qemu/general-fuzz/build/../chardev/char-fd.c:68:9
    #19 0x5651c0754736 in qio_channel_fd_source_dispatch /home/alxndr/
Development/qemu/general-fuzz/build/../io/channel-watch.c:84:12
    #20 0x7fac88fad4cd in g_main_context_dispatch (/usr/lib/x86_64-linux-
gnu/libglib-2.0.so.0+0x504cd)
    #21 0x5651c0cdfc67 in glib_pollfds_poll /home/alxndr/Development/
qemu/general-fuzz/build/../util/main-loop.c:217:9
    #22 0x5651c0cdd567 in os_host_main_loop_wait /home/alxndr/Development/
qemu/general-fuzz/build/../util/main-loop.c:240:5
    #23 0x5651c0cdcf47 in main_loop_wait /home/alxndr/Development/
qemu/general-fuzz/build/../util/main-loop.c:516:11
    #24 0x5651bf4bb08d in qemu_main_loop /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/vl.c:1676:9
    #25 0x5651bce4d51c in main /home/alxndr/Development/qemu/general-
fuzz/build/../softmmu/main.c:50:5
    #26 0x7fac887b6cc9 in __libc_start_main csu/../csu/libc-start.c:308:16
    #27 0x5651bcda2cf9 in _start (/home/alxndr/Development/qemu/general-
fuzz/build/qemu-system-i386+0x2cb0cf9)
```

```
0x61500001e500 is located 0 bytes to the right of 512-byte region
[0x61500001e300,0x61500001e500)
allocated by thread T0 here:
    #0 0x5651bce1b5b2 in calloc (/home/alxndr/Development/qemu/general-
fuzz/build/qemu-system-i386+0x2d295b2)
    #1 0x7fac88fb3210 in g_malloc0 (/usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0+0x56210)
    #2 0x5651bd8cd222 in sdhci_pci_realize /home/alxndr/Development/
qemu/general-fuzz/build/../hw/sd/sdhci-pci.c:36:5
    #3 0x5651bd88c228 in pci_qdev_realize /home/alxndr/Development/
qemu/general-fuzz/build/../hw/pci/pci.c:2114:9
    #4 0x5651c07a4ec9 in device_set_realized /home/alxndr/Development/
qemu/general-fuzz/build/../hw/core/qdev.c:864:13
    #5 0x5651bfe384b8 in property_set_bool /home/alxndr/Development/
qemu/general-fuzz/build/../qom/object.c:2202:5
    #6 0x5651bfe2c1cf in object_property_set /home/alxndr/Development/
qemu/general-fuzz/build/../qom/object.c:1349:5
    #7 0x5651bfe49471 in object_property_set_qobject /home/alxndr/
Development/qemu/general-fuzz/build/../qom/qom-qobject.c:28:10
    #8 0x5651bfe2d890 in object_property_set_bool /home/alxndr/
Development/qemu/general-fuzz/build/../qom/object.c:1416:15
    #9 0x5651c078cc64 in qdev_realize /home/alxndr/Development/
qemu/general-fuzz/build/../hw/core/qdev.c:379:12
    #10 0x5651bd8bd8cc in qdev_device_add /home/alxndr/Development/
qemu/general-fuzz/build/../qdev-monitor.c:676:10
    #11 0x5651bf4e3e43 in device_init_func /home/alxndr/Development/
qemu/general-fuzz/build/../softmmu/vl.c:2101:11
    #12 0x5651c0af71e4 in qemu_opts_foreach /home/alxndr/Development/
qemu/general-fuzz/build/../util/qemu-option.c:1172:14
    #13 0x5651bf4cd04b in qemu_init /home/alxndr/Development/qemu/general-
fuzz/build/../softmmu/vl.c:4384:5
    #14 0x5651bce4d517 in main /home/alxndr/Development/qemu/general-
fuzz/build/../softmmu/main.c:49:5
    #15 0x7fac887b6cc9 in __libc_start_main csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/alxndr/Development/
qemu/general-fuzz/build/qemu-system-i386+0x2d2893f) in __asan_memcpy
Shadow bytes around the buggy address:
  0x0c2a7fffbc50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffbc60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffbc70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffbc80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fffbc90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2a7fffbca0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffbcb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffbcc0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffbcd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffbce0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fffbcf0: 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
  Shadow gap: cc
==752161==ABORTING
```

-Alex

P J P (pjps) wrote on 2020-09-01: #1

Proposed patch
  -> https://lists.nongnu.org/archive/html/qemu-devel/2020-08/msg07968.html

Philippe Mathieu-Daudé (philmd) wrote on 2020-09-01: **[PATCH v2 3/3] hw/sd/sdhci: Fix DMA Transfer Block Size field** #4

The 'Transfer Block Size' field is 12-bit wide.

See section '2.2.2. Block Size Register (Offset 004h)' in datasheet.

Cc: <email address hidden>
Cc: Igor Mitsyanko <email address hidden>
Buglink: https://bugs.launchpad.net/qemu/+bug/1892960
Fixes: d7dfca0807a ("hw/sdhci: introduce standard SD host controller")
Reported-by: Alexander Bulekov <email address hidden>
Signed-off-by: Philippe Mathieu-Daudé <email address hidden>

Cc: <email address hidden>
---
 hw/sd/sdhci.c | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

```
diff --git a/hw/sd/sdhci.c b/hw/sd/sdhci.c
index 60f083b84c1..ecbf84e9d3f 100644
--- a/hw/sd/sdhci.c
+++ b/hw/sd/sdhci.c
@@ -1104,7 +1104,7 @@ sdhci_write(void *opaque, hwaddr offset, uint64_t
val, unsigned size)
         break;
     case SDHC_BLKSIZE:
         if (!TRANSFERRING_DATA(s->prnsts)) {
-            MASKED_WRITE(s->blksize, mask, value);
+            MASKED_WRITE(s->blksize, mask, extract32(value, 0, 12));
```

```
            MASKED_WRITE(s->blkcnt, mask >> 16, value >> 16);
        }

[...]
```

Philippe Mathieu-Daudé (philmd) wrote on 2020-10-22: #5

```
Fixed in commit dfba99f17feb6d4a129da19d38df1bcd8579d1c3.

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

Thomas Huth (th-huth) wrote on 2020-12-10: #6

```
Released with QEMU v5.2.0.

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

See full activity log

To post a comment you must log in.