[PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3

From: Philippe Mathieu-Daudé
Subject: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)
Date: Mon, 6 Sep 2021 17:31:03 +0200

```
When building QEMU with DEBUG_ATI defined then running with
'-device ati-vga,romfile="" -d unimp,guest_errors -trace ati\*'
we get:

  ati_mm_write 4 0x16c0 DP_CNTL <- 0x1
  ati_mm_write 4 0x146c DP_GUI_MASTER_CNTL <- 0x2
  ati_mm_write 4 0x16c8 DP_MIX <- 0xff0000
  ati_mm_write 4 0x16c4 DP_DATATYPE <- 0x2
  ati_mm_write 4 0x224 CRTC_OFFSET <- 0x0
  ati_mm_write 4 0x142c DST_PITCH_OFFSET <- 0xfe00000
  ati_mm_write 4 0x1420 DST_Y <- 0x3fff
  ati_mm_write 4 0x1410 DST_HEIGHT <- 0x3fff
  ati_mm_write 4 0x1588 DST_WIDTH_X <- 0x3fff3fff
  ati_2d_blt: vram:0x7fff5fa00000 addr:0 ds:0x7fff61273800 stride:2560 bpp:32
rop:0xff
  ati_2d_blt: 0 0 0, 0 127 0, (0,0) -> (16383,16383) 16383x16383 > ^
  ati_2d_blt: pixman_fill(dst:0x7fff5fa00000, stride:254, bpp:8, x:16383,
y:16383, w:16383, h:16383, xor:0xff000000)
  Thread 3 "qemu-system-i38" received signal SIGSEGV, Segmentation fault.
  (gdb) bt
  #0  0x00007ffff7f62ce0 in sse2_fill.lto_priv () at /lib64/libpixman-1.so.0
  #1  0x00007ffff7f09278 in pixman_fill () at /lib64/libpixman-1.so.0
  #2  0x0000555557b5a9af in ati_2d_blt (s=0x631000028800) at
hw/display/ati_2d.c:196
  #3  0x0000555557b4b5a2 in ati_mm_write (opaque=0x631000028800, addr=5512,
data=1073692671, size=4) at hw/display/ati.c:843
  #4  0x0000555558b90ec4 in memory_region_write_accessor (mr=0x631000039cc0,
addr=5512, ..., size=4, ...) at softmmu/memory.c:492

Commit 584acf34cb0 ("ati-vga: Fix reverse bit blts") introduced
the local dst_x and dst_y which adjust the (x, y) coordinates
depending on the direction in the SRCCOPY ROP3 operation, but
forgot to address the same issue for the PATCOPY, BLACKNESS and
WHITENESS operations, which also call pixman_fill().

Fix that now by using the adjusted coordinates in the pixman_fill
call, and update the related debug printf().

Reported-by: Qiang Liu <qiangliu@zju.edu.cn>
Fixes: 584acf34cb0 ("ati-vga: Fix reverse bit blts")
Signed-off-by: Philippe Mathieu-Daudé <philmd@redhat.com>
---
 hw/display/ati_2d.c | 6 +++---
 1 file changed, 3 insertions(+), 3 deletions(-)

diff --git a/hw/display/ati_2d.c b/hw/display/ati_2d.c
index 4dc10ea7952..692bec91de4 100644
--- a/hw/display/ati_2d.c
+++ b/hw/display/ati_2d.c
@@ -84,7 +84,7 @@ void ati_2d_blt(ATIVGAState *s)
     DPRINTF("%d %d %d, %d %d %d, (%d,%d) -> (%d,%d) %dx%d %c %c\n",
             s->regs.src_offset, s->regs.dst_offset, s->regs.default_offset,
             s->regs.src_pitch, s->regs.dst_pitch, s->regs.default_pitch,
-            s->regs.src_x, s->regs.src_y, s->regs.dst_x, s->regs.dst_y,
+            s->regs.src_x, s->regs.src_y, dst_x, dst_y,
             s->regs.dst_width, s->regs.dst_height,
             (s->regs.dp_cntl & DST_X_LEFT_TO_RIGHT ? '>' : '<'),
             (s->regs.dp_cntl & DST_Y_TOP_TO_BOTTOM ? 'v' : '^'));
@@ -180,11 +180,11 @@ void ati_2d_blt(ATIVGAState *s)
         dst_stride /= sizeof(uint32_t);
         DPRINTF("pixman_fill(%p, %d, %d, %d, %d, %d, %d, %x)\n",
                 dst_bits, dst_stride, bpp,
-                s->regs.dst_x, s->regs.dst_y,
+                dst_x, dst_y,
                 s->regs.dst_width, s->regs.dst_height,
                 filler);
         pixman_fill((uint32_t *)dst_bits, dst_stride, bpp,
-                    s->regs.dst_x, s->regs.dst_y,
+                    dst_x, dst_y,
                     s->regs.dst_width, s->regs.dst_height,
                     filler);
         if (dst_bits >= s->vga.vram_ptr + s->vga.vbe_start_addr &&
--
2.31.1
```

reply via email to
Philippe Mathieu-Daudé

[Prev in Thread] **Current Thread** [Next in Thread]

- **[PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé* **<=**
  - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Mauro Matteo Cascella*, 2021/09/06
    - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/06
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *BALATON Zoltan*, 2021/09/06
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/07
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/07
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Mauro Matteo Cascella*, 2021/09/09
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/09
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Alexander Bulekov*, 2021/09/06
      - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/07
  - **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**, *Philippe Mathieu-Daudé*, 2021/09/07

- Prev by Date: **Re: [PATCH v3 6/6] tests/qapi-schema: Test cases for aliases**
- Next by Date: **Re: [PATCH v3 0/6] qapi: Add support for aliases**
- Previous by thread: **Re: [PATCH v3 6/6] tests/qapi-schema: Test cases for aliases**
- Next by thread: **Re: [PATCH] hw/display/ati_2d: Fix buffer overflow in ati_2d_blt (CVE-2021-3638)**
- Index(es):
  - **Date**
  - **Thread**