Subject: : AmigaOS4
Topic: : The MiniGL thread
Re: The MiniGL thread
Author: : kas1e
Date: : 2019/3/20 10:46:59
URL:

@Daniel

At least one problem i can for sure 100% reproduce there : is what Petrol say, when i tried with 2.23 use force (via pressing f1 after training level) , then with 2.23 it always crashes/lockups, and with 2.20 never.

So, i use debug build with -O2 of 2.23 (only -O2, not other flags to rule optimisation out), and got nice crashlog:

```
 Crashed process: openjk_sp (0x651074F0)
DSI verbose error description: Access not allowed by page protection (protection violation)
Access was a load operation
 0: 00000086 61F6A0E0 00000002 6FFFF800 830EF160 5BB45C08 000003FC 830EDC50
 8: 00001900 C26E4122 FF0C0906 004D0D00 00000006 61F7ACD8 00000003 00000000
16: 000000FF 6FFA3420 00000000 5B61AC04 00000315 82B9A600 6FFA3420 000000AC
24: 00000100 01CC32E4 61F6A184 61F6A190 6FFFF800 00000400 5BB45C04 830EF15C
CR: 59953595   XER: E000006F  CTR: 01CC32E4  LR: 01C83508
DSISR: 00800000  DAR: 5BB45C04

FP0 : FFF80000AE124000 0000000000000000 3E7777A5C0000000 0000000000000000
FP4 : C057E67000000000 C04229D000000000 4057E67000000000 3FF2000000000000
FP8 : 4089000000000000 FFF8000000000329 C073EC9320000000 408CB64980000000
FP12: 4089485580000000 408CB64980000000 2948120531259334 CA007F24FAB0C790
FP16: 9C3107273D03CDBC 0F3511BEDD2CF8B1 0A86924B501CC9B0 BAE0887C20C24498
FP20: 4056800000000000 4330000080000000 3FF0000000000000 3F847AE147AE147B
FP24: 3FD3333333333333 0000000000000000 0000000000000000 402849BA60000000
FP28: 4070000000000000 0000000000000000 0000000000000000 3FF0000000000000
FPSCR: AE124000

Disassembly of crash site:
 01CC3538: 81240000   lwz          r9,0(r4)
 01CC353C: 38A50004   addi         r5,r5,4
 01CC3540: 38840004   addi         r4,r4,4
 01CC3544: 38C6FFFC   subi         r6,r6,4
>01CC3548: 9125FFFC   stw          r9,-4(r5)
 01CC354C: 4BFFFDE8   b            0x1CC3334
 01CC3550: 70A9001F   andi.        r9,r5,31
 01CC3554: 4182FE24   beq+         0x1CC3378
```

01CC3558: 4BFFFEA8 b 0x1CC3400
01CC355C: 7C892A78 xor r9,r4,r5

Kernel command line: serial munge debuglevel 0

Registers pointing to code:
r13: openjk_sp:cin()+0x1400 (section 25 @ 0x77F4)
r25: native kernel module graphics.library.kmod+0x000ace44
ip : native kernel module graphics.library.kmod+0x000ad0a8
lr : native kernel module graphics.library.kmod+0x0006d068
ctr: native kernel module graphics.library.kmod+0x000ace44

Stack trace:
(0x61F6A0E0) native kernel module graphics.library.kmod+0x000ad0a8
(0x61F6A140) native kernel module graphics.library.kmod+0x0006d068
(0x61F6A220) native kernel module graphics.library.kmod+0x00023ee8
(0x61F6A310) [src/texture.c:2049] LIBS:minigl.library:p96CopyBMToTex.isra.0()+0x11c (section 1 @ 0x17484)
(0x61F6A3D0) LIBS:minigl.library:cgl_GLCopyTexImage2D()+0x5d0 (section 1 @ 0x1AE6C)
(0x61F6A470) openjk_sp:_Z21RB_RenderDrawSurfListP10drawSurf_si()+0x7a0 (section 7 @ 0xAA8F4)
(0x61F6A570) openjk_sp:_Z12RB_DrawSurfsPKv()+0x94 (section 7 @ 0xAC518)
(0x61F6A5D0) openjk_sp:_Z24RB_ExecuteRenderCommandsPKv()+0xd0 (section 7 @ 0xAD944)
(0x61F6A5F0) openjk_sp:_Z21R_IssueRenderCommandsi()+0x58 (section 7 @ 0xB123C)
(0x61F6A600) openjk_sp:_Z11RE_EndFramePiS_()+0x70 (section 7 @ 0xB12C8)
(0x61F6A620) openjk_sp:_Z16SCR_UpdateScreenv()+0x104 (section 7 @ 0x13268)
(0x61F6A630) openjk_sp:_Z8CL_Frameif()+0x20c (section 7 @ 0x101BC)
(0x61F6A770) openjk_sp:_Z9Com_Framev()+0x290 (section 7 @ 0x443F8)
(0x61F6B8F0) openjk_sp:main()+0x10c (section 7 @ 0x671F4)
(0x61F6BD20) native kernel module newlib.library.kmod+0x00002520
(0x61F6BD70) native kernel module newlib.library.kmod+0x000031e4
(0x61F6BF20) native kernel module newlib.library.kmod+0x00003558
(0x61F6BF50) openjk_sp:_start()+0x170 (section 7 @ 0x16C)
(0x61F6BF90) native kernel module dos.library.kmod+0x00026724
(0x61F6BFC0) native kernel module kernel+0x0006b268
(0x61F6BFD0) native kernel module kernel+0x0006b2b0

Disassembly of crash site:
01CC3538: 81240000 lwz r9,0(r4)
01CC353C: 38A50004 addi r5,r5,4
01CC3540: 38840004 addi r4,r4,4
01CC3544: 38C6FFFC subi r6,r6,4
>01CC3548: 9125FFFC stw r9,-4(r5)
01CC354C: 4BFFFDE8 b 0x1CC3334
01CC3550: 70A9001F andi. r9,r5,31
01CC3554: 4182FE24 beq+ 0x1CC3378
01CC3558: 4BFFFEA8 b 0x1CC3400
01CC355C: 7C892A78 xor r9,r4,r5
Stack pointer (0x61F6A0E0) is inside bounds
Redzone is OK (4)

68k register dump
DATA: 843FD600 00000000 00000000 00000000 00000000 00000000 00000000 00000000

ADDR: 6FFA4000 83313D00 00000000 00000000 00000000 00000000 00000000 61F56690
Page information:
Page 0xEFA6E870:
Virtual Address: 0x5BB45000
Physical Address: 0x1A18A000
Lock count: 1
Flags (0x102): (Swappable) (Mapped)
Protection bits (0x0): (super state only)
Page is assigned to VMArea primary heap

So its cgl_GLCopyTexImage2D, and src/texture.c:2049. Can it be something about changes done lately in favor to fix Capehill's fix ?

Maybe, the same issue cause effects on others ones like light saber, etc