
Subject: : AmigaOS4

Topic: : The MiniGL thread

Re: The MiniGL thread

Author: : kas1e

Date: : 2019/3/17 11:32:01

URL:

@Capehill

Tried to reproduce it hard now , and can't from first try. Then, i keep about 5 instances working on the screen, and go to street for a hour, then when i back , they all crashes, with the same crash which i catch yesterday.

There is:

Quote:

```
[HAL_DfltTrapHandler] *** Warning: Fatal exception in task 0x5C2C4040 (Background CLI, etask = 0xEFD0CCC0) at ip 0x0181D6A0
```

```
Dump of context at 0xEFA023E0
```

```
Trap type: DSI exception
```

```
Exception Syndrome Register (ESR): 0x00000000
```

```
Machine State (raw): 0x0002F030
```

```
Machine State (verbose): [Critical Ints on] [ExtInt on] [User] [FPU on] [IAT on] [DAT on]
```

```
DSISR: 00000000 DAR: ABADCAFE
```

```
No matching page found
```

```
Temporary stack trace:
```

```
#0: in module kernel+0x0001D6A0 (0x0181D6A0)
```

```
#1: in module kernel+0x0001D7B8 (0x0181D7B8)
```

```
#2: in module kernel+0x00023604 (0x01823604)
```

```
#3: in module RadeonHD.chip+0x000A4524 (0x01D918E4)
```

```
#4: in module RadeonHD.chip+0x00015C14 (0x01D02FD4)
```

```
#5: 0x7F2971CC
```

```
#6: 0x7F4DFED0
```

```
#7: 0x7F2D95A4
```

```
#8: 0x7F9922F4
```

```
#9: 0x7F9930F4
```

```
#10: in module newlib.library.kmod+0x00002520 (0x01A82780)
```

```
#11: in module newlib.library.kmod+0x00003234 (0x01A83494)
```

```
#12: in module newlib.library.kmod+0x00003558 (0x01A837B8)
```

```
#13: 0x7F990B98
```

```
#14: in module dos.library.kmod+0x00026724 (0x0197D824)
```

```
#15: in module kernel+0x0006B268 (0x0186B268)
```

```
#16: in module kernel+0x0006B2B0 (0x0186B2B0)
```

Crashed process: testgl (0x5C2C4040)

DSI verbose error description: Page not found in hash table (page fault)

Access not allowed by page protection (protection violation)

Access was a load operation

0: 0181D7B8 5A603990 00000002 4275E5E8 4275E5E8 5ECD99C0 42765C78 00ED02C0
8: 00006FEB ABADCAFE 80000010 00005937 00000324 590CF2C8 00000230 00000000
16: 01FFFF00 01FFFF00 43F00000 0000F043 00100000 65D60000 42765C78 00000010
24: 6FFFE300 4275E5E8 02160000 00ED02C0 01823604 021828D4 4275E5E8 ABADCAFE
CR: 55355995 XER: A00007E CTR: 0181D770 LR: 0181D7B8
DSISR: 00000000 DAR: ABADCAFE

FP0 : FFF8000082004000 0000000000000000 0000000000000000 0000000000000000
FP4 : 3FF0000000000000 0000000000000000 0000000000000000 0000000000000000
FP8 : 0000000000000000 0000000000000000 0000000000000000 43300000800001E0
FP12: 4330000080000280 4330000080000280 6948120531A11314 CA405F207AB0C790
FP16: 9C3115273903CDBC 0F1446FB74B3E2C4 8A86924B501CC9B0 BAE0887C20C24498
FP20: 283740041C6A08E2 8A20756F9592D1F4 1260825EF540E830 0900422EF334C827
FP24: 993E64BE746B60D0 8C763E0261FAD873 2844AB831AC9312E 1114DEB6D0B674B1
FP28: 89FB1696DD96BCF3 4014000000000000 0000000000000000 3FF0000000000000
FPSCR: 82004000

Disassembly of crash site:

0181D690: 90010024 stw r0,36(r1)
0181D694: 93A10014 stw r29,20(r1)
0181D698: 93E1001C stw r31,28(r1)
0181D69C: 83E30000 lwz r31,0(r3)
>0181D6A0: 813F0000 lwz r9,0(r31)
0181D6A4: 2F890000 cmpwi cr7,r9,0
0181D6A8: 41DE005C beq- cr7,0x181D704
0181D6AC: 3FA00200 lis r29,512
0181D6B0: 3BBD5ECC addi r29,r29,24268
0181D6B4: 913E0000 stw r9,0(r30)

Kernel command line: serial munge debuglevel 0

Registers pointing to code:

r0 : native kernel module kernel+0x0001d7b8
r26: native kernel module kernel+0x00960000
r28: native kernel module kernel+0x00023604
r29: native kernel module kernel+0x009828d4
ip : native kernel module kernel+0x0001d6a0
lr : native kernel module kernel+0x0001d7b8
ctr: native kernel module kernel+0x0001d770

Stack trace:

(0x5A603990) native kernel module kernel+0x0001d6a0
(0x5A6039B0) native kernel module kernel+0x0001d7b8
(0x5A6039D0) native kernel module kernel+0x00023604
(0x5A603A10) native kernel module RadeonHD.chip+0x000a4524

(0x5A603A30) native kernel module RadeonHD.chip+0x00015c14
(0x5A603A50) module LIBS:Warp3D/HWdrivers/W3D_SI.library at 0x7F2971CC (section 0 @ 0x41A8)
(0x5A603B00) LIBS:Warp3D.library:_Warp3D_W3D_ClearBuffers()+0x174 (section 1 @ 0x1ECC)
(0x5A603B20) module LIBS:minigl.library at 0x7F2D95A4 (section 0 @ 0x6580)
(0x5A603B40) testgl:RunGLTest()+0x52c (section 7 @ 0x18C8)
(0x5A603CA0) testgl:main()+0x2d8 (section 7 @ 0x26C8)
(0x5A603D20) native kernel module newlib.library.kmod+0x00002520
(0x5A603D70) native kernel module newlib.library.kmod+0x00003234
(0x5A603F20) native kernel module newlib.library.kmod+0x00003558
(0x5A603F50) testgl:_start()+0x170 (section 7 @ 0x16C)
(0x5A603F90) native kernel module dos.library.kmod+0x00026724
(0x5A603FC0) native kernel module kernel+0x0006b268
(0x5A603FD0) native kernel module kernel+0x0006b2b0

Disassembly of crash site:

```
0181D690: 90010024 stw      r0,36(r1)
0181D694: 93A10014 stw      r29,20(r1)
0181D698: 93E1001C stw      r31,28(r1)
0181D69C: 83E30000 lwz      r31,0(r3)
>0181D6A0: 813F0000 lwz      r9,0(r31)
0181D6A4: 2F890000 cmpwi   cr7,r9,0
0181D6A8: 41DE005C beq-   cr7,0x181D704
0181D6AC: 3FA00200 lis     r29,512
0181D6B0: 3BBD5ECC addi   r29,r29,24268
0181D6B4: 913E0000 stw      r9,0(r30)
```

Stack pointer (0x5A603990) is inside bounds

Redzone is OK (4)

68k register dump

```
DATA: 00000001 00000000 00000000 00000000 00000000 00000000 00000000 00000000
----> 00000001 - "testgl" Hunk 0000 Offset 00000000 (SegList: 0x1982EB25)
ADDR: 6FFA4000 8325A400 00000000 00000000 00000000 00000000 00000000 5A603620
Page information:
Page not found
```

As you can see ABADCAFE in DAR , which mean we have accessed uninitialized memory.

Stack trace point out in end of all on Warp3DNova, but that can be and SDL itself which cause that, and MiniGL, and Nova itself..

I will try now to just run 2 instances and keep they working for a while.