
Subject: : Odyssey

Topic: : Odyssey 1.23 progress: r5 beta07

Re: Odyssey 1.23 progress

Author: : samo79

Date: : 2020/3/13 14:38:43

URL:

@kas1e

Got today a different kind of crash when loading a page

[https://www.ilmessaggero.it/italia/cor ... 2 marzo 2020-5107321.html](https://www.ilmessaggero.it/italia/cor...2_marzo_2020-5107321.html)

Atleast compared to usual crashes this one seems more identifiable

Quote:

Crash log for task "Odyssey"

Generated by GrimReaper 53.19

Crash occurred in module kernel at address 0x0181653C

Type of crash: DSI (Data Storage Interrupt) exception

Alert number: 0x80000003

Register dump:

GPR (General Purpose Registers):

0: 01818474 53D4F410 00000000 020B973C 3AE17000 00000000 53D4F4C8 0000001C

8: 00000000 00000000 580C27C0 00000000 24222824 53F740AC 00000000 00000000

16: 4FBB2840 FFFFFFFF 00000085 6E682D3C 53D4F738 000001C0 4962CAF8 00000000

24: 53D4F538 5FFF9300 3AE17008 3AE17018 3AE17000 00000000 020B973C 580C27C0

FPR (Floating Point Registers, NaN = Not a Number):

0: nan 0 0 0

4: 1 0 0 0

8: 0 0 13 4

12: 4.5036e+15 13 0 -0

16: 0 0 0 0

20: 0 0 0 1.61895e-319

24: 0 0 2.65249e-315 0

28: 0 13 0 0

FPSCR (Floating Point Status and Control Register): 0xB6F04100

—SPRs (Special Purpose Registers):

Machine State (msr) : 0x0002F030
Condition (cr) : 0x43DD9394
Instruction Pointer (ip) : 0x0181653C
Xtended Exception (xer) : 0x541D7018
Count (ctr) : 0x5FF724D0
Link (lr) : 0x6FB4F920
DSI Status (dsisr) : 0x541D6DD0
Data Address (dar) : 0x01A854C8

680x0 emulated registers:

DATA: 5847258E 00000003 00000000 00000000 00000000 00000000 00000000 00000000
ADDR: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 53D511B0
FPU0: 0 0 0 0
FPU4: 0 0 0 0

Symbol info:

Instruction pointer 0x0181653C belongs to module "kernel" (HUNK/Kickstart)

Stack trace:

native kernel module kernel+0x0001653c
native kernel module kernel+0x000185fc
LIBS:pthread.library:_impl_mutex_lock()+0x70 (section 1 @ 0x293C)
[source/linklib/lib.c:429] Odyssey:pthread_mutex_lock()+0x2c (section 1 @ 0x2762614)
Odyssey:_cairo_scaled_font_freeze_cache()+0x40 (section 1 @ 0x19D4B34)
Odyssey:cairo_scaled_font_text_to_glyphs()+0x254 (section 1 @ 0x19D74DC)
Odyssey:cairo_scaled_font_text_extents()+0x64 (section 1 @ 0x19D7AD0)
Odyssey:_ZN7WebCore14SimpleFontData12platformInitEv()+0x130 (section 1 @ 0x143B94)
Odyssey:_ZN7WebCore14SimpleFontDataC1ERKNS_16FontPlatformDataEbbb()+0xf0 (section 1 @ 0x140150)
Odyssey:_ZN7WebCore17CSSFontFaceSource11getFontDataERKNS_15FontDescriptionEbbPNS_15CSSFontSelectorE()+0x9ec (section 1 @ 0x15D3704)
Odyssey:_ZN7WebCore11CSSFontFace11getFontDataERKNS_15FontDescriptionEbb()+0x128 (section 1 @ 0x15D17C0)
Odyssey:_ZN7WebCore20CSSSegmentedFontFace11getFontDataERKNS_15FontDescriptionE()+0x2b0 (section 1 @ 0x1043F8C)
Odyssey:_ZN7WebCore15CSSFontSelector11getFontDataERKNS_15FontDescriptionERKN3WTF12AtomicStringE()+0xec (section 1 @ 0xFECB1C)
Odyssey:_ZN7WebCore9FontCache11getFontDataERKNS_15FontDescriptionERiPNS_12FontSelectorE()+0xd0 (section 1 @ 0x135038)
Odyssey:_ZNK7WebCore10FontGlyphs17realizeFontDataAtERKNS_15FontDescriptionEj()+0x9c (section 1 @ 0xE85CD0)
Odyssey:_ZN7WebCore12RenderInline27updateAlwaysCreateLineBoxesEb()+0x858 (section 1 @ 0x803628)
Odyssey:_ZN7WebCore11RenderBlock20layoutInlineChildrenEbRNS_10LayoutUnitES2_()+0xd18 (section 1 @ 0x7835BC)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0x438 (section 1 @

0x75F090)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock23layoutPositionedObjectsEbb()+0x1d0 (section 1 @ 0x751A80)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0x624 (section 1 @ 0x75F27C)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore17RenderFlexibleBox22layoutAndPlaceChildrenERNS_10LayoutUnitERKN3WTF6VectorIPNS_9RenderBoxELj0ENS3_15CrashOnOverflowEEERKNS4_IS1_Lj0ES7_EES1_bRNS4_INS0_11LineContextELj0ES7_EE()+0x468 (section 1 @ 0x7DE11C)

Odyssey:_ZN7WebCore17RenderFlexibleBox15layoutFlexItemsEbRN3WTF6VectorINS0_11LineContextELj0ENS1_15CrashOnOverflowEEE()+0x1f4 (section 1 @ 0x7DF294)

Odyssey:_ZN7WebCore17RenderFlexibleBox11layoutBlockEbNS_10LayoutUnitE()+0x454 (section 1 @ 0x7DFCE8)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)

Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)

Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)

Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)

Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)
Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore17RenderFlexibleBox22layoutAndPlaceChildrenERNS_10LayoutUnitERKN3WTF6VectorIPNS_9RenderBoxELj0ENS3_15CrashOnOverflowEEERKNS4_IS1_Lj0ES7_EES1_bRNS4_INS0_11LineContextELj0ES7_EE()+0x468 (section 1 @ 0x7DE11C)
Odyssey:_ZN7WebCore17RenderFlexibleBox15layoutFlexItemsEbRN3WTF6VectorINS0_11LineContextELj0ENS1_15CrashOnOverflowEEE()+0x1f4 (section 1 @ 0x7DF294)
Odyssey:_ZN7WebCore17RenderFlexibleBox11layoutBlockEbNS_10LayoutUnitE()+0x454 (section 1 @ 0x7DFCE8)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)
Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)
Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)
Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore11RenderBlock16layoutBlockChildEPNS_9RenderBoxERNS0_10MarginInfoERNS_10LayoutUnitES6_()+0x25c (section 1 @ 0x75D2C8)
Odyssey:_ZN7WebCore11RenderBlock19layoutBlockChildrenEbRNS_10LayoutUnitE()+0x1c8 (section 1 @ 0x75EA8C)
Odyssey:_ZN7WebCore11RenderBlock11layoutBlockEbNS_10LayoutUnitE()+0xaf8 (section 1 @ 0x75F750)
Odyssey:_ZN7WebCore11RenderBlock6layoutEv()+0x74 (section 1 @ 0x73A1BC)
Odyssey:_ZN7WebCore10RenderView13layoutContentERKNS_11LayoutStateE()+0x34 (section 1 @ 0x8D4F70)
Odyssey:_ZN7WebCore10RenderView6layoutEv()+0x170 (section 1 @ 0x8D5394)

Odyssey:_ZN7WebCore9FrameView6layoutEb.localalias.55()+0xd60 (section 1 @ 0x6C8EEC)
Odyssey:_ZN7WebCore9FrameView37updateLayoutAndStyleIfNeededRecursiveEv.localalias.53()+0x160
(section 1 @ 0x6CA650)
Odyssey:_ZN14WebViewPrivate8onExposeEi()+0x678 (section 1 @ 0xDDEBC)
Odyssey:_ZN7WebView8onExposeEi()+0x48 (section 1 @ 0xBA690)
Odyssey:_ZL22handleMM_OWBAApp_ExposeP6IClassPmP4_Msg()+0x1f4 (section 1 @ 0x4B54)
Odyssey:_ZL8dispatchP6IClassPmP4_Msg()+0xe44 (section 1 @ 0x1063C)
native kernel module intuition.library.kmod+0x00021448
native kernel module intuition.library.kmod+0x000215ec
native kernel module intuition.library.kmod+0x0000a3f4
native kernel module intuition.library.kmod+0x0000a034
Odyssey:_Z9main_loopv()+0x1bc (section 1 @ 0x13F4)
Odyssey:main()+0x1f0 (section 1 @ 0x1674)
native kernel module newlib.library.kmod+0x000020ac
native kernel module newlib.library.kmod+0x00002d5c
native kernel module newlib.library.kmod+0x00002ef0
Odyssey:_start()+0x170 (section 1 @ 0x214)
native kernel module dos.library.kmod+0x000255c8
native kernel module kernel+0x0003e7b4
native kernel module kernel+0x0003e7fc

PPC disassembly:

```
01816534: 81240000 lwz      r9,0(r4)
01816538: 81440004 lwz      r10,4(r4)
*0181653c: 91490004 stw      r10,4(r9)
01816540: 81240004 lwz      r9,4(r4)
01816544: 81440000 lwz      r10,0(r4)
```

System information:

CPU

Model: AMCC PPC440EP V1.3

CPU speed: 799 MHz

FSB speed: 133 MHz

Extensions:

Machine

Machine name: Sam440EP

Memory: 1048576 KB

Extensions: bus.pci