Subject: : AmigaOS4
Topic: : Updater won't run
Re: Updater won't run
Author: : Raziel
Date: : 2020/12/5 7:45:58
URL:

@Paul

Dump of context at 0xDF839BA0
Trap type: DSI exception
Machine State (raw): 0x100000000200F030
Machine State (verbose): [Hyper] [ExtInt on] [User] [FPU on] [IAT on] [DAT on]
Instruction pointer: 0x7F1E7810
Crashed process: Updater (0x507FD800)
DSI verbose error description: Access not found in hash or BAT (page fault)
Access was a load operation
0: 7F1E7878 50713050 01FFFFFF 6FF3D000 80000009 00000001 00000001 FFD4D4D4
8: 61787BD4 00000000 FFA9A9A8 02020D7C 26444884 54665260 00000012 00000000
16: 50714C20 00000018 4DD7F240 4DD7F300 00000018 000000AD 00000006 00000005
24: 4DD80000 80000009 00000001 00000012 00000000 4D96D4E0 80000002 4D96D44C
CR: 26444888 XER: 2000007F CTR: 022E42A4 LR: 7F1E7878
DSISR: 40000000 DAR: 6122257C

FP0 : FFF8000082004000 FFD5D5D5FFD5D5D5 FFD5D5D5FFD5D5D5 00C9C8C800C9C8C8
FP4 : FFD1D1D1FFD1D1D1 FFFEFCF9FFFCF9F6 FFD5D5D5FFD5D5D5 FFD5D5D5FFD5D5D5
FP8 : FFD5D5D5FFD5D5D5 433000008000002B 3FF0000000000000 4330000080000000
FP12: 4038000000000000 41E0000000000000 0000000000000000 0000000000000000
FP16: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
FP20: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
FP24: 0000000000000000 0000000000000000 0000000000000000 0000000000000000
FP28: 0000000000000000 0000000000000000 0000000000000000 8000000000000000
FPSCR: 82004000
HID0: 0x8000000000000000 HID1: 0x000000005CE993B1
HID4: 0x4400240000080180 HID5: 0x0000006600000080

V0 : 00000000000000000000000000000000 08090A0B0C0D0E0F1011121314151617
V2 : 00FF00FF00FF00FF00FF00FF00FF00FF 00FF00FF00FF00FF00FF00FF00FF00FF
V4 : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF D52BD52BD52BD52BD52BD52BD52BD52B
V6 : FE01D42BFE01D42BFE01D42BFE01D42B 00000000101010102020202030303303
V8 : 00000000000000000000000000000000 00FF00FF00FF00FF00FF00FF00FF00FF
V10: FFD5D5D5FFD5D5D50101010101010101 00000000101010102020202030303303
V12: FE01D42BFE01D42B00FF00FF00FF00FF FFD5D5D5FFD5D5D5FFD5D5D5FFD5D5D5

V14: 00100212041406160818 0A1A0C1C0E1E 0100010001000100010001000100
V16: FF000000FF000000FF000000FF000000 01010101010101010101010101010101
V18: 00000000000000000000000000000000 00000000000000000000000000000000
V20: 00000000000000000000000000000000 00000000000000000000000000000000
V22: 00000000000000000000000000000000 00000000000000000000000000000000
V24: 00000000000000000000000000000000 00000000000000000000000000000000
V26: 00000000000000000000000000000000 00000000000000000000000000000000
V28: 00000000000000000000000000000000 00000000000000000000000000000000
V30: 00000000000000000000000000000000 00000000000000000000000000000000
VSCR: 00000000 VRSAVE: 00000000

Disassembly of crash site:
```
 7F1E7800: 39000000   li          r8,0
 7F1E7804: 91010020   stw         r8,32(r1)
 7F1E7808: 810A0004   lwz         r8,4(r10)
 7F1E780C: 54EA083C   rlwinm      r10,r7,1,0,30
>7F1E7810: 7D48522E   lhzx        r10,r8,r10
 7F1E7814: 90C10010   stw         r6,16(r1)
 7F1E7818: 90810008   stw         r4,8(r1)
 7F1E781C: 7FA4EB78   mr          r4,r29
 7F1E7820: 9141001C   stw         r10,28(r1)
 7F1E7824: 90A10018   stw         r5,24(r1)
```

Kernel command line: serial debuglevel=0

Registers pointing to code:
r0 : CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x3e0 (section 1 @ 0x6854)
r5 : module APPDIR:AmiSphereServer at 0x00000001 (section 0 @ 0xFFFFFFDC)
r6 : module APPDIR:AmiSphereServer at 0x00000001 (section 0 @ 0xFFFFFFDC)
r11: native kernel module kernel+0x00020d7c
r18: CLASSES:gadgets/listviewer.gadget:Classes()+0x0 (section 8 @ 0xFFFFFFFC)
r19: CLASSES:gadgets/listviewer.gadget:IGraphics()+0x0 (section 10 @ 0xC)
r26: module APPDIR:AmiSphereServer at 0x00000001 (section 0 @ 0xFFFFFFDC)
ip : CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x378 (section 1 @ 0x67EC)
lr : CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x3e0 (section 1 @ 0x6854)
ctr: native kernel module graphics.library.kmod+0x00014824

Stack trace:
(0x50713050) CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x378 (section 1 @ 0x67EC)
(0x507130F0) CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x3e0 (section 1 @ 0x6854)
(0x507131B0) CLASSES:gadgets/listviewer.gadget:myBuffer_UpdateAll()+0x34 (section 1 @ 0x6F30)
(0x507131C0) CLASSES:gadgets/listviewer.gadget:myDispatch()+0x10c0 (section 1 @ 0x434C)
(0x507132C0) native kernel module intuition.library.kmod+0x00021448
(0x50713320) native kernel module intuition.library.kmod+0x000215ec
(0x507133A0) native kernel module intuition.library.kmod+0x0000a3f4
(0x507133B0) native kernel module intuition.library.kmod+0x0000a034
(0x50713420) CLASSES:gadgets/listviewer.gadget:myDispatch()+0x152c (section 1 @ 0x47B8)
(0x50713520) native kernel module intuition.library.kmod+0x00021448
(0x50713580) native kernel module intuition.library.kmod+0x000215ec
(0x50713600) native kernel module intuition.library.kmod+0x0000a3f4
(0x50713610) module CLASSES:gadgets/layout.gadget at 0x7FDD1B80 (section 5 @ 0x5B5C)

(0x50713730) module CLASSES:gadgets/layout.gadget at 0x7FDD95A4 (section 5 @ 0xD580)
(0x50713790) module CLASSES:gadgets/layout.gadget at 0x7FDD55E8 (section 5 @ 0x95C4)
(0x50713930) native kernel module intuition.library.kmod+0x00021448
(0x50713990) native kernel module intuition.library.kmod+0x000215ec
(0x50713A10) native kernel module intuition.library.kmod+0x0000a3f4
(0x50713A20) module CLASSES:gadgets/layout.gadget at 0x7FDD1B80 (section 5 @ 0x5B5C)
(0x50713B40) module CLASSES:gadgets/layout.gadget at 0x7FDD95A4 (section 5 @ 0xD580)
(0x50713BA0) module CLASSES:gadgets/layout.gadget at 0x7FDD55E8 (section 5 @ 0x95C4)
(0x50713D40) native kernel module intuition.library.kmod+0x00021448
(0x50713DA0) native kernel module intuition.library.kmod+0x000215ec
(0x50713E20) native kernel module intuition.library.kmod+0x0000a3f4
(0x50713E30) module CLASSES:gadgets/layout.gadget at 0x7FDD1B80 (section 5 @ 0x5B5C)
(0x50713F50) module CLASSES:gadgets/layout.gadget at 0x7FDD95A4 (section 5 @ 0xD580)
(0x50713FB0) module CLASSES:gadgets/layout.gadget at 0x7FDD55E8 (section 5 @ 0x95C4)
(0x50714150) native kernel module intuition.library.kmod+0x00021448
(0x507141B0) native kernel module intuition.library.kmod+0x000215ec
(0x50714230) native kernel module intuition.library.kmod+0x0000a3f4
(0x50714240) module CLASSES:gadgets/layout.gadget at 0x7FDD7260 (section 5 @ 0xB23C)
(0x50714290) module CLASSES:gadgets/layout.gadget at 0x7FDD95A4 (section 5 @ 0xD580)
(0x507142F0) module CLASSES:gadgets/layout.gadget at 0x7FDD8804 (section 5 @ 0xC7E0)
(0x50714370) native kernel module intuition.library.kmod+0x00021448
(0x507143D0) native kernel module intuition.library.kmod+0x000215ec
(0x50714450) native kernel module intuition.library.kmod+0x0000a3f4
(0x50714460) module CLASSES:gadgets/clicktab.gadget at 0x7F9A5B88 (section 5 @ 0x4B64)
(0x507145B0) module CLASSES:gadgets/clicktab.gadget at 0x7F9A8100 (section 5 @ 0x70DC)
(0x50714670) native kernel module intuition.library.kmod+0x00021448
(0x507146D0) native kernel module intuition.library.kmod+0x000215ec
(0x50714750) native kernel module intuition.library.kmod+0x0000a3f4
(0x50714760) module CLASSES:gadgets/layout.gadget at 0x7FDD1B80 (section 5 @ 0x5B5C)
(0x50714880) module CLASSES:gadgets/layout.gadget at 0x7FDD95A4 (section 5 @ 0xD580)
(0x507148E0) module CLASSES:gadgets/layout.gadget at 0x7FDD55E8 (section 5 @ 0x95C4)
(0x50714A80) native kernel module intuition.library.kmod+0x00021448
(0x50714AE0) native kernel module intuition.library.kmod+0x000215ec
(0x50714B60) native kernel module intuition.library.kmod+0x000219a0
(0x50714BD0) native kernel module intuition.library.kmod+0x0000e8d4
(0x50714C10) native kernel module intuition.library.kmod+0x0000eb10
(0x50714CA0) native kernel module intuition.library.kmod+0x0007fad8
(0x50714D70) module CLASSES:window.class at 0x7FDE27D8 (section 5 @ 0x87B4)
(0x50714F60) module CLASSES:window.class at 0x7FDE3AE4 (section 5 @ 0x9AC0)
(0x50715270) native kernel module intuition.library.kmod+0x00021448
(0x507152D0) native kernel module intuition.library.kmod+0x000215ec
(0x50715350) native kernel module intuition.library.kmod+0x0000a3f4
(0x50715360) native kernel module intuition.library.kmod+0x0000a034
(0x507153D0) [Updater.c:9408] Updater:make_window()+0x1564 (section 1 @ 0x20014)
(0x50715650) [Updater.c:14163] Updater:System_Startup()+0x480 (section 1 @ 0x2D378)
(0x507158B0) [Updater.c:14383] Updater:main()+0x324 (section 1 @ 0x2DADC)
(0x50715D00) native kernel module newlib.library.kmod+0x000020a4
(0x50715D70) native kernel module newlib.library.kmod+0x00002d54
(0x50715F10) native kernel module newlib.library.kmod+0x00002ee8
(0x50715F50) Updater:_start()+0x170 (section 1 @ 0x16C)
(0x50715F90) native kernel module dos.library.kmod+0x000255c8

(0x50715FC0) native kernel module kernel+0x000420ac
(0x50715FD0) native kernel module kernel+0x000420f4

Disassembly of crash site:
```
 7F1E7800: 39000000   li          r8,0
 7F1E7804: 91010020   stw         r8,32(r1)
 7F1E7808: 810A0004   lwz         r8,4(r10)
 7F1E780C: 54EA083C   rlwinm      r10,r7,1,0,30
>7F1E7810: 7D48522E   lhzx        r10,r8,r10
 7F1E7814: 90C10010   stw         r6,16(r1)
 7F1E7818: 90810008   stw         r4,8(r1)
 7F1E781C: 7FA4EB78   mr          r4,r29
 7F1E7820: 9141001C   stw         r10,28(r1)
 7F1E7824: 90A10018   stw         r5,24(r1)
```
Stack pointer (0x50713050) is inside bounds
Redzone is OK (4)

68k register dump
```
DATA: 96551C00 00000000 00000000 00000000 00000000 00000000 00000000 00000000
ADDR: 6FFB8700 96551C00 00000000 00000000 00000000 00000000 00000000 50712C30
```
Page information:
Page 0xDFCC06F0:
Virtual Address: 0x61222000
Physical Address: 0x00000000
Lock count: 0
Flags (0x800): (Guard)
Protection bits (0x0): (super state only)
Page is assigned to VMArea primary heap

I get a crash here aswell.
One that takes the system down so hard, that not even Grimmy can get up his chair.

Serial tells what is going on, though.
Seems listviewer.gadget is bombing...wasn't that updated lately?