Subject: : AmigaOS4
Topic: : Updater locking up
Re: Updater locking up
Author: : kas1e
Date: : 2021/1/9 10:17:25
URL:

@All
And there you go, i catch a crashlog when lockup another time on the running of updater:

```
 kernel 54.31 (5.1.2021) AmigaOne X5000 release
Machine model: 9 (AmigaOne X5000/20)
Dump of context at 0xEFD4C7C0
Trap type: DSI exception
DSISR: 00000000  DAR: 67FF97A4
Page: 0xEFE06360 (Virtual: 0x67FF9000, Physical: 0x00000000, Flags: 0x 800)
Machine State (raw): 0x0002F030
Machine State (verbose): [Critical Ints on] [ExtInt on] [User] [IAT on] [DAT on]
Instruction pointer: 0x7F2B47F0
Crashed process: Updater (0x60024610)
DSI verbose error description: Access to address 0x67FF97A4 not allowed by page protection in user state (
protection violation)
Access was a load operation
Exception Syndrome Register: 0x00000000
 0: 7F2B4858 54AF07D0 00000002 6FFFF800 80000009 00000001 00000001 FFD4D4D4
 8: 6855EDFC 00000000 FFA9A9A8 00006FEC 39555935 5A957234 00000010 00000000
16: 54AF1F90 00000016 650394C0 65039580 00000016 000000A5 00000006 00000005
24: 65040000 80000009 00000001 00000010 00000000 60904140 80000002 609040AC
CR: 39555999   XER: A000007E  CTR: 01C06180  LR: 7F2B4858

Disassembly of crash site:
 7F2B47E0: 39000000   li          r8,0
 7F2B47E4: 91010020   stw         r8,32(r1)
 7F2B47E8: 810A0004   lwz         r8,4(r10)
 7F2B47EC: 54EA083C   rlwinm      r10,r7,1,0,30
>7F2B47F0: 7D48522E   lhzx        r10,r8,r10
 7F2B47F4: 90C10010   stw         r6,16(r1)
 7F2B47F8: 90810008   stw         r4,8(r1)
 7F2B47FC: 7FA4EB78   mr          r4,r29
 7F2B4800: 9141001C   stw         r10,28(r1)
 7F2B4804: 90A10018   stw         r5,24(r1)
msr: 0x0002B032
TLB1 (64 entries):
```

* [52]: size=7 tid = 0 TS = 1 epn=0xFE000000 rpn=0x0000000F_FE000000 WIMG=0x5 XXWWRR=0xF protected
* [53]: size=6 tid = 0 TS = 1 epn=0x01000000 rpn=0x00000000_01000000 WIMG=0x0 XXWWRR=0x5 protected
* [54]: size=6 tid = 0 TS = 1 epn=0x01400000 rpn=0x00000000_01400000 WIMG=0x0 XXWWRR=0x5 protected
* [55]: size=6 tid = 0 TS = 1 epn=0x01800000 rpn=0x00000000_01800000 WIMG=0x0 XXWWRR=0x33 protected
* [56]: size=6 tid = 0 TS = 1 epn=0x01C00000 rpn=0x00000000_01C00000 WIMG=0x0 XXWWRR=0x33 protected
* [57]: size=6 tid = 0 TS = 1 epn=0x02000000 rpn=0x00000000_02000000 WIMG=0x0 XXWWRR=0xF protected
* [58]: size=4 tid = 0 TS = 1 epn=0x02400000 rpn=0x00000000_02400000 WIMG=0x0 XXWWRR=0xF protected
* [59]: size=3 tid = 0 TS = 1 epn=0x02440000 rpn=0x00000000_02440000 WIMG=0x0 XXWWRR=0xF protected
* [60]: size=3 tid = 0 TS = 1 epn=0x02450000 rpn=0x00000000_02450000 WIMG=0x0 XXWWRR=0xF protected
* [61]: size=7 tid = 0 TS = 0 epn=0xFE000000 rpn=0x0000000F_FE000000 WIMG=0x5 XXWWRR=0xF protected
* [62]: size=A tid = 0 TS = 0 epn=0x00000000 rpn=0x00000000_00000000 WIMG=0x0 XXWWRR=0x3F protected
* [63]: size=A tid = 0 TS = 0 epn=0x40000000 rpn=0x00000000_40000000 WIMG=0x0 XXWWRR=0x3F protected
HAL_MaxTLB = 51, HAL_NextTLB = 0
MMUCFG = 0x064809C4
mas0 = 0x103F0000
mas1 = 0xC0000A00
mas2 = 0x40000000
mas3 = 0x4000003F
mas4 = 0x00000100
mas5 = 0x00000000
mas6 = 0x00000001
mas7 = 0x00000000
mas8 = 0x00000000

Kernel command line: serial munge debuglevel=1

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)
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+0x00015b60

Stack trace:
(0x54AF07D0) CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x378 (section 1 @ 0x67EC)

(0x54AF0870) CLASSES:gadgets/listviewer.gadget:myDraw_Column()+0x3e0 (section 1 @ 0x6854)
(0x54AF0930) CLASSES:gadgets/listviewer.gadget:myBuffer_UpdateAll()+0x34 (section 1 @ 0x6F30)
(0x54AF0940) CLASSES:gadgets/listviewer.gadget:myDispatch()+0x10c0 (section 1 @ 0x434C)
(0x54AF0A40) native kernel module intuition.library.kmod+0x00020288
(0x54AF0AA0) native kernel module intuition.library.kmod+0x00021578
(0x54AF0B20) native kernel module intuition.library.kmod+0x0000a568
(0x54AF0B90) CLASSES:gadgets/listviewer.gadget:myDispatch()+0x152c (section 1 @ 0x47B8)
(0x54AF0C90) native kernel module intuition.library.kmod+0x00020288
(0x54AF0CF0) native kernel module intuition.library.kmod+0x00021578
(0x54AF0D70) module CLASSES:gadgets/layout.gadget at 0x7FDF0F2C (section 0 @ 0x5F08)
(0x54AF0E90) module CLASSES:gadgets/layout.gadget at 0x7FDF4058 (section 0 @ 0x9034)
(0x54AF0FC0) native kernel module intuition.library.kmod+0x00020288
(0x54AF1020) native kernel module intuition.library.kmod+0x00021578
(0x54AF10A0) module CLASSES:gadgets/layout.gadget at 0x7FDF0F2C (section 0 @ 0x5F08)
(0x54AF11C0) module CLASSES:gadgets/layout.gadget at 0x7FDF4058 (section 0 @ 0x9034)
(0x54AF12F0) native kernel module intuition.library.kmod+0x00020288
(0x54AF1350) native kernel module intuition.library.kmod+0x00021578
(0x54AF13D0) module CLASSES:gadgets/layout.gadget at 0x7FDF0F2C (section 0 @ 0x5F08)
(0x54AF14F0) module CLASSES:gadgets/layout.gadget at 0x7FDF4058 (section 0 @ 0x9034)
(0x54AF1620) native kernel module intuition.library.kmod+0x00020288
(0x54AF1680) native kernel module intuition.library.kmod+0x00021578
(0x54AF1700) module CLASSES:gadgets/layout.gadget at 0x7FDF7554 (section 0 @ 0xC530)
(0x54AF1760) module CLASSES:gadgets/layout.gadget at 0x7FDF6B60 (section 0 @ 0xBB3C)
(0x54AF17F0) native kernel module intuition.library.kmod+0x00020288
(0x54AF1850) native kernel module intuition.library.kmod+0x00021578
(0x54AF18D0) module CLASSES:gadgets/clicktab.gadget at 0x7FAE7E2C (section 0 @ 0x4E08)
(0x54AF1A20) module CLASSES:gadgets/clicktab.gadget at 0x7FAEA060 (section 0 @ 0x703C)
(0x54AF1AD0) native kernel module intuition.library.kmod+0x00020288
(0x54AF1B30) native kernel module intuition.library.kmod+0x00021578
(0x54AF1BB0) module CLASSES:gadgets/layout.gadget at 0x7FDF0F2C (section 0 @ 0x5F08)
(0x54AF1CD0) module CLASSES:gadgets/layout.gadget at 0x7FDF4058 (section 0 @ 0x9034)
(0x54AF1E00) native kernel module intuition.library.kmod+0x00020288
(0x54AF1E60) native kernel module intuition.library.kmod+0x00020cd8
(0x54AF1F30) native kernel module intuition.library.kmod+0x0000c290
(0x54AF1F80) native kernel module intuition.library.kmod+0x0000d410
(0x54AF2010) native kernel module intuition.library.kmod+0x0007d2c4
(0x54AF20E0) module CLASSES:window.class at 0x7FE05514 (section 0 @ 0xD4F0)
(0x54AF22B0) native kernel module intuition.library.kmod+0x00020288
(0x54AF2310) native kernel module intuition.library.kmod+0x00021578
(0x54AF2390) native kernel module intuition.library.kmod+0x0000a568
(0x54AF2400) [GUI.c:657] Updater:make_window()+0x1558 (section 1 @ 0x4308)
(0x54AF2670) [Main.c:2340] Updater:System_Startup()+0x4f4 (section 1 @ 0xD414)
(0x54AF28D0) [Main.c:2560] Updater:main()+0x32c (section 1 @ 0xDB78)
(0x54AF2D20) native kernel module newlib.library.kmod+0x000025fc
(0x54AF2D70) native kernel module newlib.library.kmod+0x000032d8
(0x54AF2F20) native kernel module newlib.library.kmod+0x0000384c
(0x54AF2F50) Updater:_start()+0x170 (section 1 @ 0x16C)
(0x54AF2F90) native kernel module dos.library.kmod+0x0002a458
(0x54AF2FC0) native kernel module kernel+0x0005c18c
(0x54AF2FD0) native kernel module kernel+0x0005c204

```
Disassembly of crash site:
 7F2B47E0: 39000000   li          r8,0
 7F2B47E4: 91010020   stw         r8,32(r1)
 7F2B47E8: 810A0004   lwz         r8,4(r10)
 7F2B47EC: 54EA083C   rlwinm      r10,r7,1,0,30
>7F2B47F0: 7D48522E   lhzx        r10,r8,r10
 7F2B47F4: 90C10010   stw         r6,16(r1)
 7F2B47F8: 90810008   stw         r4,8(r1)
 7F2B47FC: 7FA4EB78   mr          r4,r29
 7F2B4800: 9141001C   stw         r10,28(r1)
 7F2B4804: 90A10018   stw         r5,24(r1)
Stack pointer (0x54AF07D0) is inside bounds
Redzone is OK (4)

68k register dump
DATA: 81AB4700 00000000 00000000 00000000 00000000 00000000 00000000 00000000
ADDR: 6FFA4000 8157D700 00000000 00000000 00000000 00000000 00000000 54AF0430
Page information:
Page 0xEFE06360:
Virtual Address: 0x67FF9000
Physical Address: 0x00000000
Lock count: 0
Flags (0x800): (Guard)
Protection bits (0x0): (super state only)
Page is assigned to VMArea primary heap
```

See, it crashes in the listviewer.gadget:myDraw_Column()+0x378. So it faults of the listviewer.gadget which under Enhancer's hands. The version of listviewer.gadget i use are 53.29 (06/05/2020).

I do not know what version of listviewer.gadget is in public, but at least the latest one cause that issue.