
Subject: : AmigaOS4

Topic: : Markdown Editor / Viewer

Re: Markdown Editor / Viewer

Author: : kas1e

Date: : 2021/1/5 14:02:26

URL:

@billyfish

Yeah versions exactly the same as yours.

As for what .md cause crash : just download http://os4depot.net/share/utility/text/edit/vim_mui.lha

There is README.md. Load it, and click "Update" it then crashes in the HTMLview, in the DecoderThreadPC function, with 8x00000003.

Crashlog saying it can't load vimlogo.gif , and assmebler instruction which crashing is "lwz r14,12(r15)", and r14 are 0xFFFFFFFF, and r15 are 0x000000.

There is full crashlog

kernel 54.30 (1.1.2021) AmigaOne X5000 release

Machine model: 9 (AmigaOne X5000/20)

Dump of context at 0xEFA97000

Trap type: DSI exception

DSISR: 00000000 DAR: 0000000C

No matching page found

Machine State (raw): 0x0002F030

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

Instruction pointer: 0x7CCB50B0

Crashed process: HTMLview - <https://github.com/vim/vim/blob/master/runtime/vimlogo.gif> (0x5DD7D7B0)

DSI verbose error description: Access to address 0x0000000C not allowed by page protection in user state (protection violation)

Access was a load operation

Exception Syndrome Register: 0x00000000

0: 5D07AF20 5C93CD90 00000002 5C93CE30 6842DF50 01955038 FFFFFFFF 5CD53DF8

8: 5DD7D834 68430000 5E24CE24 6FEB3228 00000000 0000000D FFFFFFFF 00000000

16: 5EAF0D70 5C93CF90 7CCB568C 7CCB0000 5C93CDA0 6842DE0E 68430000 7CCBE330

24: 7CCC0000 FFFFFFFF 0239ECC2 00000000 5CD53DF8 5DD7D7B0 02008624 5CD53CC8

CR: 33953395 XER: E000007E CTR: 7CCB4FBC LR: 7CCB50A4

Disassembly of crash site:

7CCB50A0: 480109C9 bl 0x7CCC5A68

7CCB50A4: 3C806843 lis r4,26691

```
7CCB50A8: 81E10104 lwz r15,260(r1)
7CCB50AC: 3884DF50 subi r4,r4,8368
>7CCB50B0: 81CF000C lwz r14,12(r15)
7CCB50B4: 820F0000 lwz r16,0(r15)
7CCB50B8: 91C100FC stw r14,252(r1)
7CCB50BC: 818F0014 lwz r12,20(r15)
7CCB50C0: 80700000 lwz r3,0(r16)
7CCB50C4: 80AC0004 lwz r5,4(r12)
```

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:

r4 : LIBS:mui/HTMLview.mcc:_ZSt7nothrow()+0x0 (section 11 @ 0x54)

r5 : native kernel module dos.library.kmod+0x0002a458

r18: LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0x6d0 (section 1 @ 0x28688)
r19: LIBS:mui/HTMLview.mcc:_ZN13ColourManagerC2EP6Screen()+0x298 (section 1 @ 0x22FFC)
r21: module LIBS:mui/HTMLview.mcc at 0x6842DE0E (section 3 @ 0x4E)
r23: LIBS:mui/HTMLview.mcc:__gxx_personality_sj0()+0x0 (section 1 @ 0x3132C)
r24: LIBS:mui/HTMLview.mcc:__cxa_rethrow()+0x3c (section 1 @ 0x32FFC)
r26: native kernel module kernel+0x00b9ecc2
r30: native kernel module kernel+0x00808624
ip : LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0xf4 (section 1 @ 0x280AC)
lr : LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0xe8 (section 1 @ 0x280A0)
ctr: LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0x0 (section 1 @ 0x27FB8)

Stack trace:

(0x5C93CD90) LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0xf4 (section 1 @ 0x280AC)
(0x5C93CF90) LIBS:mui/HTMLview.mcc:_Z13DecoderThreadPc()+0xe8 (section 1 @ 0x280A0)
(0x5C93CFC0) native kernel module kernel+0x0005c18c
(0x5C93CFD0) native kernel module kernel+0x0005c204

Disassembly of crash site:

7CCB50A0: 480109C9 bl 0x7CCC5A68
7CCB50A4: 3C806843 lis r4,26691
7CCB50A8: 81E10104 lwz r15,260(r1)
7CCB50AC: 3884DF50 subi r4,r4,8368
>7CCB50B0: 81CF000C lwz r14,12(r15)
7CCB50B4: 820F0000 lwz r16,0(r15)
7CCB50B8: 91C100FC stw r14,252(r1)
7CCB50BC: 818F0014 lwz r12,20(r15)
7CCB50C0: 80700000 lwz r3,0(r16)
7CCB50C4: 80AC0004 lwz r5,4(r12)

Stack pointer (0x5C93CD90) is inside bounds

Redzone is OK (4)

68k register dump

DATA: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
ADDR: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Page information:

Page not found

Ready Tasks

HID Mouse (pri 10, sigrec 0x80000000, sigwait 0x80001000, masked 0x80000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
WinFrame 2 Process (pri 5, sigrec 0x00800000, sigwait 0xFF800000, masked 0x00800000)
WinFrame 3 Process (pri 5, sigrec 0x00800000, sigwait 0xFF800000, masked 0x00800000)
IDF1/FastFileSystem 53.2 (pri 5, sigrec 0x20000000, sigwait 0xA8000100, masked 0x20000000)
IDF0/FastFileSystem 53.2 (pri 5, sigrec 0x20000000, sigwait 0xA8000100, masked 0x20000000)
compose.task (pri 1, sigrec 0x00000010, sigwait 0x00000010, masked 0x00000010)
Workbench (pri 1, sigrec 0x80000100, sigwait 0x80000000, masked 0x80000000)
ScreenBlanker Library. (pri 1, sigrec 0x14000100, sigwait 0xB4001000, masked 0x14000000)
AmiDock (pri 0, sigrec 0x00000100, sigwait 0x00000100, masked 0x00000100)
NotificationServer (pri 0, sigrec 0x04000000, sigwait 0xBC001000, masked 0x04000000)
Odyssey (pri 0, sigrec 0x11000080, sigwait 0x03E0D000, masked 0x01000000)
TCP/IP Control (pri 0, sigrec 0x40000100, sigwait 0xF8009080, masked 0x40000000)

hub.usbfd (pri 0, sigrec 0x10000000, sigwait 0x30000000, masked 0x10000000)
ELF Collector (pri 0, sigrec 0x00000100, sigwait 0x00000100, masked 0x00000100)
vsata disk changer (pri 0, sigrec 0x80000000, sigwait 0x80000000, masked 0x80000000)
hub.usbfd (pri 0, sigrec 0x10000000, sigwait 0x30000000, masked 0x10000000)
dos_signal_server (pri -5, sigrec 0x00004000, sigwait 0x0000F000, masked 0x00004000)
CPUDock_idleTask (pri -127, sigrec 0x00000000, sigwait 0x40000000, masked 0x00000000)
idle.task (pri -128, sigrec 0x00000000, sigwait 0x00000000, masked 0x00000000)

Waiting Tasks

DH1/NGFileSystem 54.72 (pri 10, sigrec 0x00000100, sigwait 0xF0000000, masked 0x00000000)
)
DH0/NGFileSystem 54.72 (pri 10, sigrec 0x00000100, sigwait 0xF0000000, masked 0x00000000)
)
DH4/NGFileSystem 54.72 (pri 10, sigrec 0x00000100, sigwait 0xF0000000, masked 0x00000000)
)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
EHCI Controller Task Unit 0 (pri 15, sigrec 0x00000000, sigwait 0xBE009000, masked 0x00000000)
USB stack (pri 18, sigrec 0x00000000, sigwait 0xF800D000, masked 0x00000000)
HID Mouse (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
EHCI Controller Task Unit 1 (pri 15, sigrec 0x00000000, sigwait 0xBE009000, masked 0x00000000)
AmiMarkdown (pri 0, sigrec 0x40000000, sigwait 0x02000000, masked 0x00000000)
dopus_clock (pri 1, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
p50x0sata.device Port 1 (pri 12, sigrec 0x10000000, sigwait 0xC0007000, masked 0x00000000)
rhd_gc (pri 100, sigrec 0x00000000, sigwait 0x80000001, masked 0x00000000)
ICD1/CDFileSystem 53.8 (pri 10, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
ICD0/CDFileSystem 53.8 (pri 10, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
USB0/CrossDOSFileSystem 53.11 (pri 10, sigrec 0x00000000, sigwait 0x00010100,
masked 0x00000000)
DH2/SmartFilesystem 1.293 (pri 11, sigrec 0x00000000, sigwait 0x00000100,
masked 0x00000000)
URL/launch-handler 53.39 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
TEXTCLIP/textclip-handler 53.4 (pri 3, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
)
RANDOM/Random-Handler 52.1 (pri 5, sigrec 0x00000000, sigwait 0x00000100,
masked 0x00000000)
DH2/SmartFilesystem 1.293 (pri 10, sigrec 0x00000000, sigwait 0xE0000100,
masked 0x00000000)
MainUSB0/CrossDOSFileSystem 53.11 (pri 10, sigrec 0x00000000, sigwait 0x40000100,
masked 0x00000000)
appdir envarc manager (pri -50, sigrec 0x00000000, sigwait 0x80005000, masked 0x00000000)
Mounter Task (pri -1, sigrec 0x00000000, sigwait 0xB0001000, masked 0x00000000)
Mounter GUI (pri 0, sigrec 0x00000000, sigwait 0x80007000, masked 0x00000000)
Mounter Companion Process (pri -1, sigrec 0x00000000, sigwait 0x80003000,
masked 0x00000000)
Workbench DosList Notify (pri 1, sigrec 0x00000100, sigwait 0x00003000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
ClickToFront (pri 21, sigrec 0x00000100, sigwait 0xE000D000, masked 0x00000000)
Background CLI (pri 0, sigrec 0x00000100, sigwait 0x5C009000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
HID Keyboard (pri 10, sigrec 0x00000000, sigwait 0x90001000, masked 0x00000000)
TCP/IP Superserver (pri 0, sigrec 0x00000100, sigwait 0xD0000080, masked 0x00000000)

P50x0 Ethernet (pri 20, sigrec 0x00000000, sigwait 0x00001000, masked 0x00000000)
ContextMenus (pri 0, sigrec 0x00000000, sigwait 0xE0001000, masked 0x00000000)
Background CLI (pri 0, sigrec 0x00000100, sigwait 0xC0009000, masked 0x00000000)
dos_filedir_notify (pri 5, sigrec 0x80000000, sigwait 0x40001000, masked 0x00000000)
p50x0sata.device Port 0 (pri 12, sigrec 0x10000000, sigwait 0xC0007000, masked 0x00000000)
AmiMarkdown (pri 0, sigrec 0x40000000, sigwait 0x02000000, masked 0x00000000)
ramlib.support (pri -2, sigrec 0x00000000, sigwait 0x80005000, masked 0x00000000)
ramlib (pri 1, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
TCP/IP Configuration (pri 0, sigrec 0x00000100, sigwait 0xF8003000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
Shell Process (pri 0, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xB8000100, masked 0x00000000)
HTMLview - https:
//github.com/vim/vim/blob/master/runtime/vimlogo.gif (pri -1, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
AmiMarkdown (pri 0, sigrec 0x40000000, sigwait 0x02000000, masked 0x00000000)
[OWB] Timer (pri 0, sigrec 0x20000000, sigwait 0x50000000, masked 0x00000000)
TextEditor.mcc clipboard server (pri 1, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
dopus_arbiter (pri 0, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
sys:utilities/UnArc (pri 0, sigrec 0x00000100, sigwait 0xC0003000, masked 0x00000000)
[OWB] IconDatabase (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
RAM/ram-handler 54.24 (pri 10, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
[OWB] JavaScriptCore::BlockFree (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xB0000100, masked 0x00000000)
application.library messageserver (pri 0, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
MUI imagespace screen notify (pri 1, sigrec 0x00000100, sigwait 0xC0001000, masked 0x00000000)
RexxMaster (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
ContextMenus Command Dispatcher (pri 1, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
KeymapSwitcher.docky (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
AsyncWB (pri 0, sigrec 0x00000100, sigwait 0xC0001000, masked 0x00000000)
dopus_hotkeez (pri 1, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
RAWBInfo (pri 0, sigrec 0x00000100, sigwait 0x80001000, masked 0x00000000)
FKey (pri 0, sigrec 0x00000100, sigwait 0xC000D000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
Deflcons (pri 0, sigrec 0x00000100, sigwait 0x80009000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
Workbench Clipboard Server (pri 1, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
? IPrefs ? (pri 0, sigrec 0x20000000, sigwait 0x0000F000, masked 0x00000000)
TCP/IP Log (pri 0, sigrec 0x00000000, sigwait 0x80003000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)

ConClip (pri 0, sigrec 0x00000000, sigwait 0x80000000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
HID Keyboard (pri 10, sigrec 0x00000000, sigwait 0x90001000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
diskimage.device unit 1 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
diskimage.device unit 0 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
diskimage.device unit 5 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
diskimage.device unit 4 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
USB stack Process (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
AUDIO/AHI-Handler 6.2 (pri 5, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
APPDIR/appdir-handler 54.17 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)

MassStorage Notifier (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DST watcher (pri 0, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
NotifyA Server (pri 1, sigrec 0x00000000, sigwait 0xE8001000, masked 0x00000000)
string.gadget server (pri 1, sigrec 0x00000100, sigwait 0x40000000, masked 0x00000000)
datatypes.library (pri 1, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
ENV/env-handler 54.18 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
RAW/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
SFS DosList handler (pri 19, sigrec 0x00000000, sigwait 0x80000000, masked 0x00000000)
dos_nbmd_process (pri 5, sigrec 0x00000000, sigwait 0x00001100, masked 0x00000000)
dos_lock_handler (pri 5, sigrec 0x00000000, sigwait 0x00001100, masked 0x00000000)
hub.usbfd (pri 0, sigrec 0x00000000, sigwait 0x30000000, masked 0x00000000)
hub.usbfd (pri 0, sigrec 0x00000000, sigwait 0x30000000, masked 0x00000000)

Exec Command and Control (pri 30, sigrec 0x00000000, sigwait 0x80000000,

masked 0x00000000)

DMA2 Channel 4 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 4 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 3 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 3 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 2 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 2 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 1 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 1 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)

Suspended Tasks