

---

Subject: : AmigaOS4

Topic: : Porting to AmigaOS4 thread

Re: Porting to AmigaOS4 thread

Author: : Capehill

Date: : 2019/4/4 17:55:18

URL:

@Raziel

Debugged little bit more and put a trap instruction inside dead canary detector. It seems that there is some bitmap freed:

Quote:

(0x64D93E40) [engines/fullpipe/fullpipe.cpp:162] scummvm:free()+0x1a4 (section 8 @ 0x236C8)  
(0x64D93E90) [engines/fullpipe/fullpipe.cpp:162] scummvm:free()+0x1a4 (section 8 @ 0x236C8)  
(0x64D93EC0) [engines/fullpipe/gfx.cpp:715] scummvm:\_ZN8Fullpipe6BitmapD1Ev()+0x50 (section 8 @ 0x36EE8)  
(0x64D93EE0) scummvm:\_ZN6Common14DefaultDeleterIN8Fullpipe6BitmapEEclEPS2\_()+0x38 (section 8 @ 0x3D548)  
(0x64D93F00) [engines/fullpipe/gfx.cpp:255]  
scummvm:\_ZN6Common9ScopedPtrIN8Fullpipe6BitmapENS\_14DefaultDeleterIS2\_EEE5resetEPS2\_()+0x34 (section 8 @ 0x3D59C)  
(0x64D93F30) [engines/fullpipe/gfx.cpp:422] scummvm:\_ZN8Fullpipe7Picture11freePictureEv()+0xf0 (section 8 @ 0x375BC)  
(0x64D93F50) [engines/fullpipe/gfx.cpp:412] scummvm:\_ZN8Fullpipe7PictureD2Ev()+0x30 (section 8 @ 0x377C0)  
(0x64D93F70) scummvm:\_ZN8Fullpipe11StaticPhaseD2Ev()+0x44 (section 8 @ 0xA47C8)  
(0x64D93F90) scummvm:\_ZN8Fullpipe12DynamicPhaseD2Ev()+0x34 (section 8 @ 0xA482C)  
(0x64D93FB0) scummvm:\_ZN8Fullpipe7StaticsD0Ev()+0x54 (section 8 @ 0xA48B0)  
(0x64D93FD0) scummvm:\_ZN6Common14DefaultDeleterIN8Fullpipe7StaticsEEclEPS2\_()+0x44 (section 8 @ 0xA3A58)  
(0x64D93FF0) [engines/fullpipe/statics.cpp:145]  
scummvm:\_ZN6Common8for\_eachIPPIN8Fullpipe7StaticsENS\_14DefaultDeleterIS2\_EEEET0\_T\_S8\_S7\_()+0x44 (section 8 @ 0xA3AB4)  
(0x64D94010) [engines/fullpipe/statics.cpp:115] scummvm:\_ZN8Fullpipe15StaticANIOBJECTD0Ev()+0x68 (section 8 @ 0xA21E0)  
(0x64D94030) [engines/fullpipe/scene.cpp:124] scummvm:\_ZN8Fullpipe5SceneD0Ev()+0x118 (section 8 @ 0x84BBC)  
(0x64D94060) [engines/fullpipe/gameloader.cpp:421]  
scummvm:\_ZN8Fullpipe10GameLoader11unloadSceneEi()+0xf8 (section 8 @ 0x2BB44)  
(0x64D94090) [engines/fullpipe/gameloader.cpp:387]  
scummvm:\_ZN8Fullpipe10GameLoader12preloadSceneEii()+0x254 (section 8 @ 0x2CB2C)

——(0x64D940F0) [engines/fullpipe/gameloader.cpp:572]  
scummvm:\_ZN8Fullpipe10GameLoader13updateSystemsEi()+0xc8 (section 8 @ 0x2CDC4)  
(0x64D94110) [engines/fullpipe/modal.cpp:233] scummvm:\_ZN8Fullpipe10ModallIntro6finishEv()+0xc4  
(section 8 @ 0x62268)  
(0x64D94130) [engines/fullpipe/modal.cpp:91] scummvm:\_ZN8Fullpipe10ModallIntro4initEi()+0x54 (section  
8 @ 0x64198)  
(0x64D94170) [engines/fullpipe/fullpipe.cpp:630]  
scummvm:\_ZN8Fullpipe14FullpipeEngine12updateScreenEv()+0x13c (section 8 @ 0x24000)  
(0x64D94190) [engines/fullpipe/fullpipe.cpp:440] scummvm:\_ZN8Fullpipe14FullpipeEngine3runEv()+0x5b8  
(section 8 @ 0x25394)  
(0x64D94320) [base/main.cpp:327]  
scummvm:\_Z7runGamePK6PluginR7OSystemRKN6Common6StringE()+0xd48 (section 8 @ 0x80A0)  
(0x64D94840) [base/main.cpp:599] scummvm:scummvm\_main()+0xde8 (section 8 @ 0x953C)  
(0x64DDA0E0) [backends/platform/sdl/amigaos/amigaos-main.cpp:79] scummvm:main()+0x260 (section 8  
@ 0x6AF8)

It could be that heap corruption has something to do with endian issues. To fix endian issues, somebody would have to go through all file loading code in fullpipe engine.

Here is one obvious bug (but doesn't fix graphics):

<https://github.com/scummvm/scummvm/blob/master/fullpipe/utils.cpp#L260>

It gives just bogus reading for BE.