

ET: Legacy Development - Bug #1211

Segfault on client linux x64 at startup (master branch)

25.02.2019 02:50 - Ododo

Status:	New	% Done:	0%
Priority:	Normal		
Assignee:			
Category:	Client		
Target version:	2.77		
OS:	Linux	Arch:	64-bit
Description			
<pre>Starting program: /home/olivier/etlegacy/etl [Thread debugging using libthread_db enabled] Using host libthread_db library "/usr/lib/libthread_db.so.1". ET Legacy v2.76-139-g1abf64a5 linux-x86_64 Feb 25 2019 Zone megs: 64 Info: fs_game now defaults to 'legacy' mod instead of 'etmain' ----- FS_Startup ----- Current search path: /home/olivier/.etlegacy/legacy ./legacy ./legacy/pak3_v2.76_dirty.pk3 (1122 files) ./legacy/etl_bin_v2.76_dirty.pk3 (2 files) /home/olivier/.etlegacy/etmain ./etmain ./etmain/pak2.pk3 (22 files) ./etmain/pak1.pk3 (10 files) ./etmain/pak0.pk3 (3725 files) ----- 4881 files in pk3 files SQLite3 libversion 3.26.0 - database URI 'etl.db' - in file ... loading existing database '/home/olivier/.etlegacy/etl.db' ... database file '/home/olivier/.etlegacy/etl.db' loaded SQLite3 ETL: DB init #2/home/olivier/.etlegacy/etl.db in [0] ms - autocommit 1 SQLite3 ETL: DB schema version #2 is up to date! Warning: etl_pakmeta.txt was not found. execing default.cfg couldn't exec autoexec.cfg Hunk_Clear: reset the hunk ok Not logging server attacks to disk. ----- Client Initialization ----- ----- Initializing Renderer ---- Trying to load "librenderer_opengl1_x86_64.so" from "/home/olivier/etlegacy"... ----- ETKEY found. Available client translations: Bulgarian Czech German Greek English Esperanto Spanish Finnish French Hungarian Italian Korean Dutch Norwegian Polish Portuguese Romanian Russian Slovak Slovenian Serbian Swedish Turkish Available mod translations: Bulgarian Czech German Greek English Esperanto Spanish Finnish French Hungarian Italian Korean Dutch Norwegian Polish Portuguese Romanian Russian Slovak Slovenian Serbian Swedish Turkish Language set to English ----- Client Initialization Complete ----- ----- R_Init ----- SDL build version 2.0.9 - link version 2.0.9. SDL initialized driver "x11" Initializing OpenGL display Estimated display aspect: 1.781 ...setting mode -2: 1368x768 Using 24 color bits, 24 depth, 0 stencil display. Available modes [22]: '684x384 1368x768 432x243 480x270 512x288 640x360 800x450 864x486 960x540 1024x576 1280x720 160</pre>			

0x900 640x400 1280x800 700x450 1400x900 320x240 400x300 512x384 640x480 800x600 1024x768'

Using GLEW 2.1.0

GL_VENDOR: NVIDIA Corporation

GL_RENDERER: GeForce 610M/PCIe/SSE2

GL_VERSION: 4.6.0 NVIDIA 390.87

Using vanilla renderer

Initializing OpenGL extensions

...found OpenGL extension - GL_EXT_texture_compression_s3tc

...found OpenGL extension - GL_EXT_texture_env_add

...found OpenGL extension - GL_ARB_multitexture

GL_VENDOR: NVIDIA Corporation

GL_RENDERER: GeForce 610M/PCIe/SSE2

GL_VERSION: 4.6.0 NVIDIA 390.87

GL_MAX_TEXTURE_SIZE: 16384

GL_MAX_ACTIVE_TEXTURES_ARB: 4

PIXELFORMAT: color(24-bits) Z(24-bit) stencil(0-bits)

MODE: -2, SCREEN: 1368 x 768 fullscreen (ratio 1.7812) Hz:N/A

GAMMA: hardware w/ 0 overbright bits

rendering primitives: single glDrawElements

texturemode: GL_LINEAR_MIPMAP_NEAREST

picmip: 1

texture bits: 0

multitexture: enabled

compiled vertex arrays: enabled

texenv add: enabled

compressed textures: enabled

Initializing Shaders

----- finished R_Init -----

----- Initializing Sound (1)-----

SDL_Init(SDL_INIT_AUDIO)... [New Thread 0x7fffd380d700 (LWP 22078)]

OK

SDL audio driver is "pulseaudio".

[New Thread 0x7fffd37cc700 (LWP 22079)]

SDL_AudioSpec:

Format: AUDIO_S16LSB

Freq: 44100

Samples: 1024

Channels: 2

Silence: 0

Size: 4096

Starting SDL audio callback...

SDL audio initialized.

----- Sound Info -----

sound system is muted

2 channels

32768 samples

16 samplebits

1 submission_chunk

44100 speed

0x5555583dd500 dma buffer

No background file.

Sound initialization successfully done

s_backend set to SDL2

Sound memory manager started

Sys_LoadGameDll -> FS_CL_ExtractFromPakFile(/home/olivier/.etlegacy, legacy, ui.mp.x86_64.so)

Sys_LoadDll(/home/olivier/.etlegacy/legacy/ui.mp.x86_64.so)... succeeded

Sys_LoadDll(legacy/ui) found vmMain function at 0x7fffd2bd0b30

Initializing Legacy ui v2.76-139-g1abf64a5

150 UI cvars in use.

Thread 1 "etl" received signal SIGSEGV, Segmentation fault

(gdb) bt

#0 0x000055555555d6665 in PC_Directive_define.part.7 ()

#1 0x000055555555d6da1 in PC_DefineFromString ()

```
#2 0x00005555555d6eb9 in PC_AddGlobalDefine ()
#3 0x00005555555fc189 in CL_UISystemCalls ()
#4 0x00005555555cec43 in VM_DllSyscall ()
#5 0x00007fffd2bea4a4 in ?? () from /home/olivier/.etlegacy/legacy/ui.mp.x86_64.so
#6 0x00007fffd2bce494 in ?? () from /home/olivier/.etlegacy/legacy/ui.mp.x86_64.so
#7 0x00007fffd2bd056a in ?? () from /home/olivier/.etlegacy/legacy/ui.mp.x86_64.so
#8 0x00007fffd2bd0bc9 in vmMain () from /home/olivier/.etlegacy/legacy/ui.mp.x86_64.so
#9 0x00005555555cfb6b in VM_CallFunc ()
#10 0x00005555555a5f39 in Com_Init ()
#11 0x0000555555591de6 in main ()
```

History

#1 - 25.02.2019 18:05 - IR4T4

This issue is system dependant and was one of the reasons why our last release was delayed. See #1089

Which distribution is this?

#2 - 25.02.2019 18:38 - Ododo

IR4T4 wrote:

This issue is system dependant and was one of the reasons why our last release was delayed. See #1089

Which distribution is this?

This was on ArchLinux

Linux 4.19.15-rt12-1-rt #1 SMP PREEMPT RT Mon Feb 18 15:51:39 CET 2019 x86_64 GNU/Linux

EDIT: gcc --version
gcc (GCC) 8.2.1 2018112

#3 - 25.02.2019 19:39 - Spyhawk

Arch Linux is affected by the issue (even when set up as a strictly minimal system). So far, only *some* systems work when etl is build in a container. See #1089.

#4 - 28.02.2019 17:31 - Ododo

Guess for that precise segfault (not related to other 64bit build issue):

the asm instruction that segfault is movaps
movaps usually segfault on alignment issues
Occurs after GetMemory that uses Z_TagMalloc which is architecture dependant.

Maybe something has changed in common.c ?

#5 - 01.03.2019 15:14 - Spyhawk

- Target version set to 2.77