
Subject: Problem with MemorySanitizer

Posted by [Novo](#) on Sun, 21 Feb 2021 00:14:26 GMT

[View Forum Message](#) <> [Reply to Message](#)

tutorial/CoreTutorial

```
~/dvlp/cpp/code/upp/out/tutorial/CLANGcpp17msan.Debug.Debug_Full.Gui.Mt.Shared.Usemalloc
$ ./CoreTutorial
```

Uninitialized bytes in __interceptor_strlen at offset 0 inside [0x701000000b00, 11)

==31245==WARNING: MemorySanitizer: use-of-uninitialized-value

```
#0 0x7fd5730d6b5e (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xbb5e)
#1 0x7fd5730d961f in FcConfigFilename (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xe61f)
#2 0x7fd5730f3151 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x28151)
#3 0x7fd5730e4f77 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x19f77)
#4 0x7fd5730e51da (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x1a1da)
#5 0x7fd5730d7156 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xc156)
#6 0x7fd5730e52a9 in FcInitBringUptoDate
(/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x1a2a9)
#7 0x7fd5730e7ea1 in FcFontList (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x1cea1)
#8 0x259c28e in Upp::GetAllFacesSys()
/home/ssg/dvlp/cpp/code/upp/git/uppsrc/Draw/FontFc.cpp:233:18
#9 0x259ae3d in Upp::Font::FaceList()
/home/ssg/dvlp/cpp/code/upp/git/uppsrc/Draw/Font.cpp:34:10
#10 0x259df7f in Upp::sInitFonts() /home/ssg/dvlp/cpp/code/upp/git/uppsrc/Draw/Font.cpp:42:2
#11 0x259e098 in Upp::s__sF0_46_fn()
/home/ssg/dvlp/cpp/code/upp/git/uppsrc/Draw/Font.cpp:47:2
#12 0x56ad11 in Upp::Callinit::Callinit(void (*)(), char const*, int)
/home/ssg/dvlp/cpp/code/upp/git/uppsrc/Core/Defs.h:86:83
#13 0x434934 in __cxx_global_var_init.4
/home/ssg/dvlp/cpp/code/upp/git/uppsrc/Draw/Font.cpp:46:1
#14 0x434f3c in _GLOBAL__sub_I_Draw_blitz.cpp
/home/ssg/dvlp/cpp/code/upp/out/tutorial/Draw/CLANGcpp17msan.Debug.Debug_Full.Gui.Mt.Shared.Usemalloc/Draw$blitz.cpp
#15 0x2f3643c in __libc_csu_init
(/home/ssg/dvlp/cpp/code/upp/out/tutorial/CLANGcpp17msan.Debug.Debug_Full.Gui.Mt.Shared.Usemalloc/CoreTutorial+0x2f3643c)
#16 0x7fd571ba5c3d in __libc_start_main csu/../csu/libc-start.c:270:6
#17 0x43554d in _start
(/home/ssg/dvlp/cpp/code/upp/out/tutorial/CLANGcpp17msan.Debug.Debug_Full.Gui.Mt.Shared.Usemalloc/CoreTutorial+0x43554d)
```

Uninitialized value was created by a heap allocation

```
#0 0x44198d in malloc
(/home/ssg/dvlp/cpp/code/upp/out/tutorial/CLANGcpp17msan.Debug.Debug_Full.Gui.Mt.Shared.Usemalloc/CoreTutorial+0x44198d)
#1 0x7fd5730d95bf in FcConfigFilename (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xe5bf)
```

SUMMARY: MemorySanitizer: use-of-uninitialized-value

```
(/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xbb5e)
```

Exiting

Sanitizers detect problems with newly compiled code. They do not instrument binary code like valgrind does.

bm-file is attached.

File Attachments

1) [CLANGcpp17msan.bm](#), downloaded 146 times
