
Subject: Re: U++ 2019.1.rc4 released

Posted by [Novo](#) on Fri, 19 Apr 2019 22:51:44 GMT

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

I do not know who is responsible for this crash (libfontconfig.so.1+0xdb67 or /uppsrc/Draw/Font.cpp:34:10), but I cannot even get close to my own code.

Memory Sanitizer:

Uninitialized bytes in __interceptor_strlen at offset 0 inside [0x7010000008a0, 11)

==30845==WARNING: MemorySanitizer: use-of-uninitialized-value

```
#0 0x7f3bb6714097 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xb097)
#1 0x7f3bb6716baa in FcConfigFilename (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xdbaa)
#2 0x7f3bb672f607 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x26607)
#3 0x7f3bb6721be3 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x18be3)
#4 0x7f3bb6721e45 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x18e45)
#5 0x7f3bb6714736 (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xb736)
#6 0x7f3bb6721f05 in FcInitBringUptoDate
(/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x18f05)
#7 0x7f3bb6724be9 in FcFontList (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0x1bbe9)
#8 0x292ed45 in Upp::GetAllFacesSys()
/home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/FontFc.cpp:236:18
#9 0x292e354 in Upp::Font::FaceList() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:34:10
#10 0x292fc97 in Upp::sInitFonts() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:42:2
#11 0x292fd68 in Upp::s__sF0_46_fn() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:47:2
#12 0x12bb799 in Upp::Callinit::Callinit(void (*)(), char const*, int)
/home/ssg/dvlp/cpp/upp/git/uppsrc/Core/Defs.h:176:83
#13 0x469944 in __cxx_global_var_init.4
/home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:46:1
#14 0x469d5c in _GLOBAL__sub_I__blitz.cpp
/home/ssg/dvlp/cpp/upp/git/out/MyApps/Draw/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.
Usemalloc/$blitz.cpp
#15 0x3dfd874 in __libc_csu_init
(/home/ssg/dvlp/cpp/upp/git/out/MyApps/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.Use
malloc/OpenCorpora+0x3dfd874)
#16 0x7f3bb47a0029 in __libc_start_main
/build/glibc-B9XfQf/glibc-2.28/csu/./csu/libc-start.c:264:6
#17 0x471839 in _start
(/home/ssg/dvlp/cpp/upp/git/out/MyApps/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.Use
malloc/OpenCorpora+0x471839)
```

Uninitialized value was created by a heap allocation

```
#0 0x47adfc in __interceptor_malloc
(/home/ssg/dvlp/cpp/upp/git/out/MyApps/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.Use
malloc/OpenCorpora+0x47adfc)
#1 0x7f3bb6716b67 in FcConfigFilename (/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xdb67)
#2 0x292e354 in Upp::Font::FaceList() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:34:10
#3 0x292fc97 in Upp::sInitFonts() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:42:2
#4 0x292fd68 in Upp::s__sF0_46_fn() /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:47:2
#5 0x12bb799 in Upp::Callinit::Callinit(void (*)(), char const*, int)
```

```
/home/ssg/dvlp/cpp/upp/git/uppsrc/Core/Defs.h:176:83
#6 0x469944 in __cxx_global_var_init.4 /home/ssg/dvlp/cpp/upp/git/uppsrc/Draw/Font.cpp:46:1
#7 0x469d5c in _GLOBAL__sub_I__blitz.cpp
/home/ssg/dvlp/cpp/upp/git/out/MyApps/Draw/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.
Usemalloc/$blitz.cpp
#8 0x3dfd874 in __libc_csu_init
(/home/ssg/dvlp/cpp/upp/git/out/MyApps/CLANGcpp17msan.Debug.Debug_Full.Gui.Shared.Use
malloc/OpenCorpora+0x3dfd874)
```

SUMMARY: MemorySanitizer: use-of-uninitialized-value
(/usr/lib/x86_64-linux-gnu/libfontconfig.so.1+0xb097)
Exiting
