Subject: CTRL-F2 crashes on UBUNTU 12.04 64-Bit
Posted by ManfredHerr on Sun, 05 Jan 2014 22:39:58 GMT
View Forum Message <> Reply to Message

Since yesterday or so I get a TheIDE crash when I try to sync translation files. This is not dependent on the project but with example projects (home budget) as well.

I did an uninstall and and reinstall with the software center. The icon in the starter changed but the crash remained. So I fetched the debug symbols and run theide with gdb:

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff4f55fd5 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
(gdb) where
#0 0x00007ffff4f55fd5 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
#1 0x00000000006bd562 in Upp::StringBuffer::Realloc (this=0x7fffffc70a0, n=-1, cat=0x0, l=0)
at /build/buildd/upp-5485/uppsrc/Core/String.cpp:376
#2 0x00000000006bd630 in Upp::StringBuffer::SetLength (this=0x7fffffc70a0, l=-1)
at /build/buildd/upp-5485/uppsrc/Core/String.cpp:394
#3 0x00000000004a3a00 in Upp::StringBuffer::StringBuffer (this=0x7fffffc70a0, len=-1)
at uppsrc/Core/String.h:413
#4 0x00000000006d278b in Upp::LoadStream (in=...) at
/build/buildd/upp-5485/uppsrc/Core/Stream.cpp:1489
#5 0x00000000006d2899 in Upp::LoadFile (
filename=0x7fffd8eedb58 "/home/manfred/upp/examples/HomeBudget/src.tpp")
at /build/buildd/upp-5485/uppsrc/Core/Stream.cpp:1500
#6 0x000000000081e9f6 in LngParseCFile (fn=..., lng=...) at
/build/buildd/upp-5485/uppsrc/ide/t.cpp:50
#7 0x0000000000822c55 in Ide::SyncT (this=0x7fffffd4e10, kind=0)
at /build/buildd/upp-5485/uppsrc/ide/t.cpp:526
#8 0x000000000076493a in Upp::CallbackMethodActionArg<Ide, void (Ide::*)(int), int>::Execute (
this=0x7fffd8eb8240) at uppsrc/Core/Callback1.h:26
#9 0x00000000006e24a1 in Upp::Callback::Execute (this=0x7fffd8ebaea8)
at /build/buildd/upp-5485/uppsrc/Core/Callback.cpp:7
#10 0x0000000000458a1a in Upp::Callback::operator() (this=0x7fffd8ebaea8) at
uppsrc/Core/Cbgen.h:32
#11 0x00000000006e2bde in Upp::CallbackForkAction::Execute (this=0x7fffd8ebae90)
at /build/buildd/upp-5485/uppsrc/Core/Callback0.h:54
#12 0x00000000006e24a1 in Upp::Callback::Execute (this=0x7fffd8ebf260)
at /build/buildd/upp-5485/uppsrc/Core/Callback.cpp:7
#13 0x0000000000458a1a in Upp::Callback::operator() (this=0x7fffd8ebf260) at
uppsrc/Core/Cbgen.h:32
#14 0x00000000006ac777 in Upp::MenuItem::LeftUp (this=0x7fffd8ebf1c0)
at /build/buildd/upp-5485/uppsrc/CtrlLib/MenuItem.cpp:361
#15 0x00000000005bcf59 in Upp::Ctrl::MouseEvent (this=0x7fffd8ebf1c0, event=145, p=...,
zdelta=0, keyflags=0)
at /build/buildd/upp-5485/uppsrc/CtrlCore/CtrlMouse.cpp:139
#16 0x00000000005bca91 in Upp::Ctrl::MouseEventH (this=0x7fffd8ebf1c0, event=145, p=...,
zdelta=0, keyflags=0)

```
    at /build/buildd/upp-5485/uppsrc/CtrlCore/CtrlMouse.cpp:93
#17 0x00000000005bde37 in Upp::Ctrl::MEvent0 (this=0x7fffd8ebf1c0, e=145, p=..., zd=0)
    at /build/buildd/upp-5485/uppsrc/CtrlCore/CtrlMouse.cpp:296
#18 0x00000000005bfc67 in Upp::Ctrl::DispatchMouseEvent (this=0x7fffd8ebf1c0, e=145, p=...,
zd=0)
    at /build/buildd/upp-5485/uppsrc/CtrlCore/CtrlMouse.cpp:560
#19 0x00000000005bfc29 in Upp::Ctrl::DispatchMouseEvent (this=0x7ffff7e48e60, e=145, p=...,
zd=0)
    at /build/buildd/upp-5485/uppsrc/CtrlCore/CtrlMouse.cpp:560
---Type <return> to continue, or q <return> to quit---q
Quit
...
1485 String LoadStream(Stream& in) {
1486  if(in.IsOpen()) {
1487   in.ClearError();
1488   int size = (int)in.GetLeft();
1489   StringBuffer s(size);
1490   if((dword)size != 0xffffffff)
1491    in.Get(s, size);
1492   if(!in.IsError())
1493    return s;
(gdb) p size
$1 = -1
(gdb) up
#5  0x00000000006d2899 in Upp::LoadFile (
    filename=0x7fffd8eedb58 "/home/manfred/upp/examples/HomeBudget/src.tpp")
    at /build/buildd/upp-5485/uppsrc/Core/Stream.cpp:1500
1500  return LoadStream(in);
...
```

The Realloc does a memcpy with size -1 -> crash.
Load File tries to read the directory "/home/manfred/upp/examples/HomeBudget/src.tpp" that cannot be read as file. So LoadStream allocates a StringBuffer of size -1. The check of size is one statement later, too late...

Why has it already been working? I don't know.
How can it be fixed? I don't know either.

By the way, in Windows XPprof. all is fine.

PS.: I checked the update history of my machine and discovered that the Software update of Jan. 3rd contained linux-libc-dev(3.2.0-57.87, 3.2.0-58.88)

OK, changing from "stable" upp to upp-nightly did the trick. Hasn't the time come to release a newer stable version ?