
Subject: svd build - segmentation fault changing main package [bug]

Posted by [mdelfede](#) on Tue, 11 Sep 2007 10:35:40 GMT

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

On current svn build (on Ubuntu Feisty), but only on this machine (the one at home runs ok...), if I open a main package and then I change to another main package, the ide crashes with segmentation fault. I rebuilt id with debug; here the backtrace :

```
Starting program: /usr/bin/theide
[Thread debugging using libthread_db enabled]
[New Thread -1219406128 (LWP 14677)]
Writes to freed blocks detected
```

```
Program received signal SIGABRT, Aborted.
```

```
[Switching to Thread -1219406128 (LWP 14677)]
```

```
0xffffe410 in __kernel_vsyscall ()
```

```
(gdb) backtrace
```

```
#0 0xffffe410 in __kernel_vsyscall ()
```

```
#1 0xb75ffdf0 in raise () from /lib/tls/i686/cmov/libc.so.6
```

```
#2 0xb7601641 in abort () from /lib/tls/i686/cmov/libc.so.6
```

```
#3 0x083078e8 in Upp::Panic (msg=0x85a8c1c "Writes to freed blocks detected")
  at /home/massimo/sources/upp/uppsrc/Core/Util.cpp:53
```

```
#4 0x08307a22 in Upp::HeapPanic (
  text=0x85a8c1c "Writes to freed blocks detected", pos=0xb486d374, size=3)
  at /home/massimo/sources/upp/uppsrc/Core/heap.cpp:148
```

```
#5 0x08309e69 in Upp::FreeCheck (ptr=0xb486d374, count=3)
  at /home/massimo/sources/upp/uppsrc/Core/heap.cpp:163
```

```
#6 0x08309ed2 in Upp::CheckFree (p=0xb486d350, k=2)
  at /home/massimo/sources/upp/uppsrc/Core/heap.cpp:287
```

```
#7 0x0830b2c2 in Upp::MemoryAlloc (sz=40)
  at /home/massimo/sources/upp/uppsrc/Core/heap.cpp:337
```

```
#8 0x08302ed6 in Upp::MemoryAllocDebug (size=24)
  at /home/massimo/sources/upp/uppsrc/Core/heapdbg.cpp:72
```

```
#9 0x080f6e43 in operator new (size=20)
  at /home/massimo/sources/upp/uppsrc/Core/Core.h:372
```

```
#10 0x08460242 in Upp::callback<Upp::TopWindow, Upp::TopWindow> (
  object=0xbfeb0e3c, method=(void ( class Upp::TopWindow::*)(void)) 17334570)
  at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:81
```

```
#11 0x08449e60 in Upp::TopWindow::SyncTitle (this=0xbfeb0e3c)
  at /home/massimo/sources/upp/uppsrc/CtrlCore/TopWinX11.cpp:82
```

```
#12 0x0844a560 in Upp::TopWindow::Title (this=0xbfeb0e3c, _title=@0xbfeaff60)
  at /home/massimo/sources/upp/uppsrc/CtrlCore/TopWindow.cpp:309
```

```
#13 0x080a31e3 in Ide::MakeTitle (this=0xbfeb0e3c)
  at /home/massimo/sources/upp/uppsrc/ide/ide.cpp:39
```

```
#14 0x080dcfc5 in Upp::CallbackMethodAction<Ide, void (Ide::*)()>::Execute (
  this=0xb71d41a8) at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:31
```

```
#15 0x082f9e22 in Upp::Callback::Execute (this=0xbfeb1f50)
  at /home/massimo/sources/upp/uppsrc/Core/Callback.cpp:11
```

#16 0x080fb6e7 in Upp::Callback::operator() (this=0xbfef1f50)
at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:63

#17 0x081f96e3 in Upp::TextCtrl::ClearDirty (this=0xbfef1e5c)
at /home/massimo/sources/upp/uppsrc/CtrlLib/Text.cpp:160

#18 0x081f97ee in Upp::TextCtrl::Clear (this=0xbfef1e5c)
at /home/massimo/sources/upp/uppsrc/CtrlLib/Text.cpp:63

#19 0x0823d4e0 in Upp::LineEdit::Clear (this=0xbfef1e5c)
at /home/massimo/sources/upp/uppsrc/CtrlLib/LineEdit.cpp:30

#20 0x081026e1 in Upp::CodeEditor::Clear (this=0xbfef1e5c)
at /home/massimo/sources/upp/uppsrc/CodeEditor/CodeEditor.h:351

#21 0x080a5c75 in Ide::FlushFile (this=0xbfef0e3c)
at /home/massimo/sources/upp/uppsrc/ide/idefile.cpp:331

#22 0x080c9318 in Ide::SetMain (this=0xbfef0e3c, package=@0xbfef01e8)
at /home/massimo/sources/upp/uppsrc/ide/ide.cpp:118

#23 0x080d09af in Ide::OpenMainPackage (this=0xbfef0e3c)
at /home/massimo/sources/upp/uppsrc/ide/ide.cpp:171

#24 0x080d242a in Ide::NewMainPackage (this=0xbfef0e3c)
at /home/massimo/sources/upp/uppsrc/ide/ide.cpp:180

#25 0x080dcfc5 in Upp::CallbackMethodAction<Ide, void (Ide::*)()>::Execute (this=0xb4872178) at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:31

#26 0x082f9e22 in Upp::Callback::Execute (this=0xb480ad54)
at /home/massimo/sources/upp/uppsrc/Core/Callback.cpp:11

#27 0x080fb6e7 in Upp::Callback::operator() (this=0xb480ad54)
at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:63

#28 0x08335234 in Upp::CallbackForkAction::Execute (this=0xb480ad48)
at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:96

#29 0x082f9e22 in Upp::Callback::Execute (this=0xb48d6c88)
at /home/massimo/sources/upp/uppsrc/Core/Callback.cpp:11

#30 0x080fb6e7 in Upp::Callback::operator() (this=0xb48d6c88)
at /home/massimo/sources/upp/uppsrc/Core/Cbgen.h:63

#31 0x081f90f9 in Upp::MenuItem::LeftUp (this=0xb48d6c28)
at /home/massimo/sources/upp/uppsrc/CtrlLib/MenuBar.cpp:496

#32 0x084470c6 in Upp::Ctrl::MouseEvent (this=0xb48d6c28, event=145, p=@0xbfef0404, zdelta=0, keyflags=0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:131

#33 0x08450cbf in Upp::Ctrl::MouseEventH (this=0xb48d6c28, event=145, p=@0xbfef04a0, zdelta=0, keyflags=0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:87

#34 0x084512a2 in Upp::Ctrl::MouseEvent0 (this=0xb48d6c28, e=145, p=@0xbfef0590, zd=0) at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:284

#35 0x08451649 in Upp::Ctrl::DispatchMouseEvent (this=0xb48d6c28, e=145, p=@0xbfef0658, zd=0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:524

#36 0x08451608 in Upp::Ctrl::DispatchMouseEvent (this=0xb71ca7b4, e=145, p=@0xbfef0728, zd=0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:524

#37 0x08451608 in Upp::Ctrl::DispatchMouseEvent (this=0xb71ca720, e=145, p=@0xbfef0824, zd=0)

```
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:524
#38 0x08451f4d in Upp::Ctrl::DispatchMouse (this=0xb71ca720, e=145,
p=@0xbf09f0, zd=0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/CtrlMouse.cpp:503
#39 0x084534ef in Upp::Ctrl::EventProc (this=0xb71ca720, w=@0xb5211ec8,
event=0xbf0ce0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/X11Proc.cpp:315
#40 0x08456fe9 in Upp::Ctrl::ProcessEvent (event=0xbf0ce0)
at /home/massimo/sources/upp/uppsrc/CtrlCore/X11Wnd.cpp:203
#41 0x08457fe0 in Upp::Ctrl::EventLoop (ctrl=0xbf0e3c)
at /home/massimo/sources/upp/uppsrc/CtrlCore/X11Wnd.cpp:311
#42 0x08458303 in Upp::TopWindow::Run (this=0xbf0e3c, appmodal=false)
at /home/massimo/sources/upp/uppsrc/CtrlCore/TopWindow.cpp:281
#43 0x080d1e50 in GuiMainFn_ ()
at /home/massimo/sources/upp/uppsrc/ide/idewin.cpp:839
#44 0x080d23e6 in main (argc=Cannot access memory at address 0x3955
)
at /home/massimo/sources/upp/uppsrc/ide/idewin.cpp:570
(gdb)
```

Hope it will be useful.... I don't know enough (yet) about upp to find the bug by myself !

Ciao

Max

Subject: Re: svd build - segmentation fault changing main package [bug]
Posted by [mdelfede](#) on Sat, 06 Oct 2007 13:35:29 GMT
[View Forum Message](#) <> [Reply to Message](#)

Same error building uvs snapshot.

Ciao

Max

Subject: Re: svd build - segmentation fault changing main package [bug]
Posted by [mdelfede](#) on Sun, 21 Oct 2007 19:33:14 GMT
[View Forum Message](#) <> [Reply to Message](#)

Looking more in depth, the bug happens when you exit theide after the main package selection, too... so it should be easier to find, I hope.

Just a question : the `::MemoryChech()` function does a complete heap check, even the freed blocks ?

Ciao

Max

EDIT : Investigating a bit more, I found that the heap corruption happens (at first) in the function `Ide::FlushFile()` when the line `Editor.Disable()` is called. If I suppress this line, the Ide goes a bit further before crashing again.

I guess it's something inside the assist editor....
