
Subject: Re: IDE crash on loading package
Posted by [dolik.rce](#) on Fri, 13 Apr 2012 06:20:23 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi Nick,

Looks like some glitch in the Assist parser. I've been able reproduce it, just as you said - Typed "::Requested size: 2684354580 B
U++ allocated memory: 3952556 KB
It apparently falls into endless loop somewhere in the parser, adding more and more items into a Vector that holds the information about parsed code. The stack backtrace for completeness: Out of memory!
#0 0x081d32f2 in Upp::sPanicMessageBox (title=0x8587849 "Fatal error", text=0xbffe1ef4 "Out of memory!\nRequested size: 2684354580 B\nU++ allocated memory: 3952556 KB") at /build/buildd/upp-4776/uppsrc/CtrlCore/X11App.cpp:216
#1 0x082afa04 in Upp::PanicMessageBox (title=0x8587849 "Fatal error", text=0xbffe1ef4 "Out of memory!\nRequested size: 2684354580 B\nU++ allocated memory: 3952556 KB") at /build/buildd/upp-4776/uppsrc/Core/Util.cpp:24
#2 0x082afb5a in Upp::Panic (msg=0xbffe1ef4 "Out of memory!\nRequested size: 2684354580 B\nU++ allocated memory: 3952556 KB") at /build/buildd/upp-4776/uppsrc/Core/Util.cpp:50
#3 0x08291ced in Upp::OutOfMemoryPanic (size=2684354580) at /build/buildd/upp-4776/uppsrc/Core/heaputil.cpp:56
#4 0x08291d8a in Upp::SysAllocRaw (size=2684354636, reqsize=-1610612716) at /build/buildd/upp-4776/uppsrc/Core/heaputil.cpp:78
#5 0x08293423 in Upp::Heap::LAlloc (this=0x88d7700, size=@0xbffe2074) at /build/buildd/upp-4776/uppsrc/Core/lheap.cpp:160
#6 0x08292e0c in Upp::Heap::Alloc (this=0x88d7700, sz=2684354580) at /build/buildd/upp-4776/uppsrc/Core/sheap.cpp:138
#7 0x08292b6f in Upp::MemoryAlloc_ (sz=2684354580) at /build/buildd/upp-4776/uppsrc/Core/sheap.cpp:317
#8 0x08294adc in Upp::MemoryAlloc (size=2684354560) at /build/buildd/upp-4776/uppsrc/Core/heapdbg.cpp:88
#9 0x08294b9a in Upp::MemoryAllocSz (size=@0xbffe2100) at /build/buildd/upp-4776/uppsrc/Core/heapdbg.cpp:109
#10 0x082b4539 in Upp::VectorReAlloc_ (v_=0xbffe22b4, newalloc=134217728, sizeofT=20) at /build/buildd/upp-4776/uppsrc/Core/Vcont.cpp:35
#11 0x082b4624 in Upp::VectorGrow_ (v_=0xbffe22b4, sizeofT=20) at /build/buildd/upp-4776/uppsrc/Core/Vcont.cpp:55
#12 0x082b464c in Upp::VectorGrowF_ (v_=0xbffe22b4, sizeofT=20) at /build/buildd/upp-4776/uppsrc/Core/Vcont.cpp:67
#13 0x0808d055 in Upp::Vector<ItemTextPart>::GrowF (this=0xbffe22b4) at uppsrc/Core/Vcont.h:37
#14 0x0808d003 in Upp::Vector<ItemTextPart>::Add (this=0xbffe22b4) at uppsrc/Core/Vcont.h:44
#15 0x0808c822 in ParseItemNatural (name=..., m=..., s=0xb406e7b8 "::#16 0x0808cd2f in ParseItemNatural (m=..., s=0xb406e7b8 "::#17 0x0808cd75 in ParseItemNatural (m=...) at

/build/buildd/upp-4776/uppsrc/ide/Browser/Item.cpp:177
#18 0x0808dc84 in CppItemInfoDisplay::DoPaint (this=0xbffe8b58, w=..., r=..., q=..., _ink=..., paper=..., style=0) at /build/buildd/upp-4776/uppsrc/ide/Browser/ItemDisplay.cpp:14 4
#19 0x0808e66b in CppItemInfoDisplay::Paint (this=0xbffe8b58, w=..., r=..., q=..., _ink=..., paper=..., style=0) at /build/buildd/upp-4776/uppsrc/ide/Browser/ItemDisplay.cpp:19 1
#20 0x0820617c in Upp::ArrayCtrl::DoPaint (this=0xbffe961c, w=..., sample=false) at /build/buildd/upp-4776/uppsrc/CtrlLib/ArrayCtrl.cpp:839
#21 0x08206679 in Upp::ArrayCtrl::Paint (this=0xbffe961c, w=...) at /build/buildd/upp-4776/uppsrc/CtrlLib/ArrayCtrl.cpp:884
#22 0x081a7a01 in Upp::Ctrl::CtrlPaint (this=0xbffe961c, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:376
#23 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffea618, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#24 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffea68c, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#25 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffe8ae8, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#26 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffe8a54, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#27 0x081a7889 in Upp::Ctrl::CtrlPaint (this=0xbffe5994, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:355
#28 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbfff65b4, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#29 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffe590c, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#30 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbfff67b8, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#31 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbfff1e50, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#32 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbfff670c, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#33 0x081a7cca in Upp::Ctrl::CtrlPaint (this=0xbffe4314, w=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:393
#34 0x081a90aa in Upp::Ctrl::UpdateArea0 (this=0xbffe4314, draw=..., clip=..., backpaint=2) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:580
#35 0x081a942e in Upp::Ctrl::UpdateArea (this=0xbffe4314, draw=..., clip=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/CtrlDraw.cpp:612
#36 0x081c1f20 in Upp::Ctrl::DoPaint (this=0xbffe4314, invalid=...) at /build/buildd/upp-4776/uppsrc/CtrlCore/X11Wnd.cpp:66
#37 0x081c33db in Upp::Ctrl::TimerAndPaint () at /build/buildd/upp-4776/uppsrc/CtrlCore/X11Wnd.cpp:332
#38 0x081c395f in Upp::Ctrl::EventLoop0 (ctrl=0xbffe4314) at /build/buildd/upp-4776/uppsrc/CtrlCore/X11Wnd.cpp:434
#39 0x081e41bd in Upp::CallbackActionCallArg<void (*) (Upp::Ctrl*), Upp::Ctrl*, unsigned int>::Execute (this=0xb46844a0) at uppsrc/Core/Callback1.h:48
#40 0x082b6636 in Upp::Callback::Execute (this=0xbffe41dc) at /build/buildd/upp-4776/uppsrc/Core/Callback.cpp:7
#41 0x08091f9b in Upp::Callback::operator() (this=0xbffe41dc) at uppsrc/Core/Cbgen.h:32

#42 0x081e35b3 in Upp::Ctrl::Call (cb=...) at
/build/buildd/upp-4776/uppsrc/CtrlCore/CtrlMt.cpp:128
#43 0x081e3aa5 in Upp::Ctrl::EventLoop (ctrl=0xbffe4314) at
/build/buildd/upp-4776/uppsrc/CtrlCore/CtrlMt.cpp:192
#44 0x081b5f20 in Upp::TopWindow::Run (this=0xbffe4314, appmodal=false) at
/build/buildd/upp-4776/uppsrc/CtrlCore/TopWindow.cpp:327
#45 0x08329202 in GuiMainFn_ () at /build/buildd/upp-4776/uppsrc/ide/idewin.cpp:905
#46 0x08327e99 in main (argc=1, argv=0xbffff2c4, envp=0xbffff2cc) at
/build/buildd/upp-4776/uppsrc/ide/idewin.cpp:592

Honza
