

Modal Dialogs on worker threads can cause exceptions in MFC with N

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.ui/2004-09/0215.html>

From: CJ (CJ_at_newsgroup.nospam)

Date: 09/16/04

Date: Thu, 16 Sep 2004 10:15:04 -0700

I have an MFC application that puts up several message boxes on worker threads at the same time. This has always worked when compiled with MFC 6.0. We have recently upgraded this app to MFC 7.0 and 7.1 (Visual Studio .NET 2002 and Visual Studio .NET 2003). The app continues to work with no problem on Windows 2000 and Windows XP. However, it now crashes on Windows NT with SP6.

The problem seems to be related to re-entrant code inside MFC CFrameWnd. To put it in a nutshell, the main GUI thread calls into CFrameWnd::BeginModalState, creates the m_phWndDisable array, and then gets stuck inside the ::EnableWindow(hWnd, FALSE) call a few lines later in the same function. There are then about 4 other Sent messages on the stack, and finally CFrameWnd::EndModalState() is called, which deletes the m_phWndDisable array and nulls out the pointer. The stack is then popped, and the main thread access violates when the "m_phWndDisable[nIndex] = hWnd;" line is executed.

For anyone interested I have a small application that reproduces the problem. I could not find this issue reported on any of the newsgroups - maybe we are the only ones putting up modal dialogs on worker threads?

I am also curious as to why this behavior is only seen on Windows NT. It seems from the code that this could also happen on Windows 2000 or XP. The stack dump right before this problem happened is as follows (apologies for the length!). This dump is for Visual Studio .NET 2002. The dump is similar for Visual Studio .NET 2003.

```
> mfc70d.dll!CFrameWnd::EndModalState() Line 415 C++
   mfc70d.dll!CFrameWnd::OnEnable(int bEnable=1) Line 473 C++
   mfc70d.dll!CWnd::OnWndMsg(unsigned int message=10, unsigned int wParam=1,
long lParam=0, long * pResult=0x0012f184) Line 2019 C++
   mfc70d.dll!CWnd::WindowProc(unsigned int message=10, unsigned int
wParam=1, long lParam=0) Line 1737 + 0x1e C++
   mfc70d.dll!AfxCallWndProc(CWnd * pWnd=0x00301c20, HWND__ *
hWnd=0x005f046e, unsigned int nMsg=10, unsigned int wParam=1, long lParam=0)
```

```
Line 241 + 0x1a C++
    mfc70d.dll!AfxWndProc(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=1, long lParam=0) Line 387 C++
    mfc70d.dll!AfxWndProcBase(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=1, long lParam=0) Line 209 + 0x15 C++
    USER32.DLL!77e71484()
    USER32.DLL!77e71dbb()
    NTDLL.DLL!77f76563()
    USER32.DLL!77e72b4c()
    mfc70d.dll!CWnd::SendMessageA(unsigned int message=877, unsigned int
wParam=64, long lParam=0) Line 44 + 0x42 C++
    mfc70d.dll!CFrameWnd::OnActivate(unsigned int nState=0, CWnd *
pWndOther=0x002f6e98, int bMinimized=0) Line 974 + 0x2e C++
    mfc70d.dll!CWnd::OnWndMsg(unsigned int message=6, unsigned int wParam=0,
long lParam=3278046, long * pResult=0x0012f488) Line 2092 C++
    mfc70d.dll!CWnd::WindowProc(unsigned int message=6, unsigned int wParam=0,
long lParam=3278046) Line 1737 + 0x1e C++
    mfc70d.dll!AfxCallWndProc(CWnd * pWnd=0x00301c20, HWND__ *
hWnd=0x005f046e, unsigned int nMsg=6, unsigned int wParam=0, long
lParam=3278046) Line 241 + 0x1a C++
    mfc70d.dll!AfxWndProc(HWND__ * hWnd=0x005f046e, unsigned int nMsg=6,
unsigned int wParam=0, long lParam=3278046) Line 387 C++
    mfc70d.dll!AfxWndProcBase(HWND__ * hWnd=0x005f046e, unsigned int nMsg=6,
unsigned int wParam=0, long lParam=3278046) Line 209 + 0x15 C++
    USER32.DLL!77e71484()
    USER32.DLL!77e71dbb()
    NTDLL.DLL!77f76563()
    USER32.DLL!77e72b4c()
    mfc70d.dll!CFrameWnd::NotifyFloatingWindows(unsigned long dwFlags=32)
Line 518 C++
    mfc70d.dll!CFrameWnd::OnEnable(int bEnable=0) Line 482 C++
    mfc70d.dll!CWnd::OnWndMsg(unsigned int message=10, unsigned int wParam=0,
long lParam=0, long * pResult=0x0012f774) Line 2019 C++
    mfc70d.dll!CWnd::WindowProc(unsigned int message=10, unsigned int
wParam=0, long lParam=0) Line 1737 + 0x1e C++
    mfc70d.dll!AfxCallWndProc(CWnd * pWnd=0x00301c20, HWND__ *
hWnd=0x005f046e, unsigned int nMsg=10, unsigned int wParam=0, long lParam=0)
Line 241 + 0x1a C++
    mfc70d.dll!AfxWndProc(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 387 C++
    mfc70d.dll!AfxWndProcBase(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 209 + 0x15 C++
    USER32.DLL!77e71484()
    USER32.DLL!77e71dbb()
    NTDLL.DLL!77f76563()
    USER32.DLL!77e72b4c()
    mfc70d.dll!CFrameWnd::NotifyFloatingWindows(unsigned long dwFlags=32)
Line 518 C++
    mfc70d.dll!CFrameWnd::OnEnable(int bEnable=0) Line 482 C++
    mfc70d.dll!CWnd::OnWndMsg(unsigned int message=10, unsigned int wParam=0,
long lParam=0, long * pResult=0x0012fa60) Line 2019 C++
```

```
mfc70d.dll!CWnd::WindowProc(unsigned int message=10, unsigned int
wParam=0, long lParam=0) Line 1737 + 0x1e C++
    mfc70d.dll!AfxCallWndProc(CWnd * pWnd=0x00301c20, HWND__ *
hWnd=0x005f046e, unsigned int nMsg=10, unsigned int wParam=0, long lParam=0)
Line 241 + 0x1a C++
    mfc70d.dll!AfxWndProc(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 387 C++
    mfc70d.dll!AfxWndProcBase(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 209 + 0x15 C++
    USER32.DLL!77e71484()
    USER32.DLL!77e71dbb()
    NTDLL.DLL!77f76563()
    mfc70d.dll!CFrameWnd::OnEnable(int bEnable=0) Line 467 C++
    mfc70d.dll!CWnd::OnWndMsg(unsigned int message=10, unsigned int wParam=0,
long lParam=0, long * pResult=0x0012fcf8) Line 2019 C++
    mfc70d.dll!CWnd::WindowProc(unsigned int message=10, unsigned int
wParam=0, long lParam=0) Line 1737 + 0x1e C++
    mfc70d.dll!AfxCallWndProc(CWnd * pWnd=0x00301c20, HWND__ *
hWnd=0x005f046e, unsigned int nMsg=10, unsigned int wParam=0, long lParam=0)
Line 241 + 0x1a C++
    mfc70d.dll!AfxWndProc(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 387 C++
    mfc70d.dll!AfxWndProcBase(HWND__ * hWnd=0x005f046e, unsigned int nMsg=10,
unsigned int wParam=0, long lParam=0) Line 209 + 0x15 C++
    USER32.DLL!77e71484()
    USER32.DLL!77e71dbb()
    NTDLL.DLL!77f76563()
    USER32.DLL!77e71ef1()
    mfc70d.dll!CWinThread::Run() Line 648 + 0x15 C++
    mfc70d.dll!CWinApp::Run() Line 680 C++
    mfc70d.dll!AfxWinMain(HINSTANCE__ * hInstance=0x00400000, HINSTANCE__ *
hPrevInstance=0x00000000, char * lpCmdLine=0x00132b62, int nCmdShow=1) Line
49 + 0xb C++
    TestThreadedMessageBox.exe!WinMain(HINSTANCE__ * hInstance=0x00400000,
HINSTANCE__ * hPrevInstance=0x00000000, char * lpCmdLine=0x00132b62, int
nCmdShow=1) Line 25 C++
    TestThreadedMessageBox.exe!WinMainCRTStartup() Line 392 + 0x3b C
    KERNEL32.DLL!77f1bbb5()
```

```
--
cj
```