

Re: LoadLibrary race/deadlock

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2004-11/0613.html>

From: Jonathan Morrison [MSFT] (jonathanm_at_mindspring.com)

Date: 11/25/04

Date: Wed, 24 Nov 2004 17:28:27 -0800

Can you include the callstack for that thread by using the 'k' command?

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Use of any included script samples are subject to the terms specified at

<http://www.microsoft.com/info/copyright.htm>

"Henry Markov" <jnhblhr@yahoo.com> wrote in message

news:41A4EE59.70E80BD3@yahoo.com...

> Pavel and Jonathan,

> Thanks for the responses. I've done software development for 30+ years

> but very

> little in the Windows domain therefore most of your information was new to

> me.

> Here is the log from my debug session:

>

> Opened log file 'c:\enclog'

> 0:000> !locks

>

> CritSec ntdll!LdrpLoaderLock+0 at 7C97C0D8

> LockCount 2

> RecursionCount 2

> OwningThread fd4

> EntryCount 1

> ContentionCount 1

> *** Locked

>

> Scanned 145 critical sections

> 0:000> ~~[fd4]s

> eax=00000075 ebx=000000e8 ecx=00000010 edx=0007e3e2 esi=003f22c0

> edi=000000e8

> eip=7c90eb94 esp=0012f51c ebp=0012f54c iopl=0 nv up ei pl zr na po

> nc

> cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000

> efl=00000246

> ntdll!KiFastSystemCallRet:

> 7c90eb94 c3 ret

> Closing open log file c:\enclog

>

> I suppose this verifies a deadlock but the information about thread ID fd4

> appears to be mostly register and condition code values that don't tell me

> much. Is there something in this information that is clearly important?

>

> Note that I have been told that the DLL that I am invoking does not have a

> DllMain. Does anything in the output suggest that libmmd.dll is

> implicated in

microsoft.public.win32.programmer.kernel: Re: LoadLibrary race/deadlock

```
> the deadlock? To repeat, an earlier version of the DLL compiled with VC6
> never
> exhibited this race/deadlock. It started immediately after switching to
> the
> Intel compiler which we want to use because of its Pentium-M
> optimizations. The
> Intel compiler, but not VC6, creates a dependency on libmmd.dll.
>
> HM
>
> Pavel Lebedinsky wrote:
>>
>> When the program hangs, attach to it with windbg/cdb and run
>> these commands:
>>
>> 0:000> .symfix c:\symbols
>> 0:000> .reload
>> 0:000> !locks
>>
>> Most likely your problem is caused by somebody holding the loader
>> lock, so you should see something like this in the output:
>>
>> CritSec ntdll!LdrpLoaderLock+0 at 7C97C0D8
>> LockCount          0
>> RecursionCount     1
>> OwningThread       a08
>> EntryCount         0
>> ContentionCount    0
>> *** Locked
>>
>> You can then switch to the thread that holds the lock (in this
>> case it's thread id 0xa08) and check what it is doing:
>>
>> 0:000> ~~[a08]s
>> 0:000> k
```