

# Re: Frame-based exception handling problem on Server 2008

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2008-02/msg00263.htm>

---

- *From:* "Ivan Brugiolo [MSFT]" <[ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 22 Feb 2008 15:19:33 -0800
- 

Vista SP1 and WinSrv2008 are build from the same code, and, the only SKU difference is the exception validation behavior that is triggered by the NX boot and CPU options (among other things: there are specific appcomp shims to skip exception handlers validation for binaries known to have issues).

That said, the safe exception handler table has nothing to do with C++. It's a structure referenced in the debug-directory of the PE, and it is used for exception handler validation.

Using the MS toolset, if you do

```
`link -dump -all <binary> | findstr /c:"Safe Exception Handler Table"`  
you should see that yourself.
```

To debug the issue, start from KeUserExceptionDispatcher. That's the first function you can set a breakpoint on in user mode. Then, with good symbols, observe the code that walks the frame-handler list, and, check if some Rtl\*Validate\* function is called.

—  
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>

"Corinna Vinschen" <[corinna@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:corinna@xxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:fpn0nk\\$cv7\\$2@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:fpn0nk$cv7$2@xxxxxxxxxxxxxxxxxxxxxxxx)

Hi Ivan,

Ivan Brugiolo [MSFT] wrote:

Can you elaborate on the NX options of the bcdedit configuration ?

Per the output of bcdedit, the NX option is set to OptOut.

Re: Frame-based exception handling problem on Server 2008

My take is that the server SKU has NX enabled by default, that implies strict validation of the SEH-Handler against the table generated by the compiler,  
while the client SKU has a looser validation, and your code gets by.

The compiler (GCC) does not generate SEH handlers, except if you use c++ exception handling. This is not the case here. The code is plain C.

The second problem is that our approach works as expected on 2003 Server, as well as on earlier Server versions, so it shouldn't have anything to do with server vs. client.

Anyway, I switched the 2008 Server to OptIn as in Vista and rebooted. I verified that the setting was still OptIn after the reboot. The problem that 2008 Server hangs persists even with NX=OptIn.

Then, could you use a ntsd/cdb/windbg based debugger to report the stack ?  
Those debuggers have the ability to use public PDBs to give meaningful stack traces.

I haven't windbg installed. If it's necessary, I can do that, but I never used it so I'd need some instructions. For the time being, I have pasted the backtrace from ProcessExplorer in the hanging example code from my reply to Jeffrey on a 2008 Server:

```
0 ntdll.dll!RtlTimeToElapsedTimeFields+0x12225
1 ntdll.dll!KiUserExceptionDispatcher+0xf
2 exceptionhandler_example.exe+0x13e9
3 exceptionhandler_example.exe+0x124b
4 exceptionhandler_example.exe+0x1298
5 kernel32.dll!BaseThreadInitThunk+0x12
6 ntdll.dll!RtlInitializeExceptionChain+0x63
7 ntdll.dll!RtlInitializeExceptionChain+0x36
```

Does that help?

Corinna

--

Corinna Vinschen  
Cygwin Project Co-Leader  
Red Hat

Re: Frame-based exception handling problem on Server 2008