

!heap failed in windbg. Invalid type information f

Posted by Alexei Tchernoraenko - 17 Mar 2011 - 16:32

Hello,

I'm trying to dump heap information from full dump memory file sitting on Windows Server 2003 SP2 x86.

Dump was created for 32-bit mixed (native/clr) application which was running on Windows Server 2003 SP2 x64 machine.

From the following windbg log I see that loaded ntdll.dll image is incorrect and does not correspond to ntdll.pdb symbols.

I have tried to specify the location to ntdll.dll from the target machine but windbg still shows that the module is loaded from the standard location (c:windowssystem32).

What did I do wrong? How to force windbg to load correct version of ntdll?

Microsoft (R) Windows Debugger Version 6.11.0001.404 X86

Copyright (c) Microsoft Corporation. All rights reserved.

0:042> vertarget

Windows Server 2003 Version 3790 (Service Pack 2) MP (4 procs) Free x86 compatible

Product: Server, suite: TerminalServer SingleUserTS

kernel32.dll version: 5.2.3790.4480 (srv03_sp2_gdr.090321-1244)

Machine Name:

Debug session time: Wed Mar 16 16:36:10.000 2011 (GMT-5)

System Uptime: 17 days 10:34:26.068

Process Uptime: 1 days 15:19:14.000

Kernel time: 0 days 1:24:01.000

User time: 0 days 22:07:58.000

0:042> .sympath

Symbol search path is:

C:\mscordacwksv2.0.50727.3615;C:__exe;SRV*CSymbols*http://referencesource.microsoft.com/symbols;SRV*c:Symbols*http://msdl.microsoft.com/download/symbols;SRV*C:Symbols*http://source.msdn.microsoft.com/symbols

0:042> .exepath

Executable image search path is: C:__exe;C:__target\WindowsSysWOW64;

0:042> .reload

0:042> .reload /u ntdll.dll

Unloaded ntdll.dll

0:042> .reload /v /f ntdll.dll

AddImage: C:\WINDOWS\system32\ntdll.dll // why is it still c:\windowssystem32

DllBase = 7d600000

Size = 000f0000

Checksum = 000c371a
TimeStamp = 4cc1831e

0:042> lm

7d600000 7d6f0000 ntdll (pdb symbols)
c:symbols\ntdll.pdb9ED8E09C6723448380648C4456726AEF2wntdll.pdb

0:042> !heap

*** Your debugger is not using the correct symbols ***

*** Type referenced: ntdll!_HEAP_ENTRY ***

Invalid type information

0:042> lmi vm ntdll

start end module name

7d600000 7d6f0000 ntdll (pdb symbols) ntdll.dll
Symbol file: c:symbols\ntdll.pdb9ED8E09C6723448380648C4456726AEF2wntdll.pdb
Image path: C:\WINDOWS\system32\ntdll.dll
Image name: ntdll.dll
Timestamp: Fri Oct 22 07:27:10 2010 (4CC1831E)
CheckSum: 000C371A
ImageSize: 000F0000
File version: 5.2.3790.4789 // this is correct and correspond to target computer
Product version: 5.2.3790.4789
File flags: 0 (Mask 3F)
File OS: 40004 NT Win32
File type: 2.0 Dll
File date: 00000000.00000000
Translations: 0409.04b0
CompanyName: Microsoft Corporation
ProductName: Microsoft Windows Operating System
InternalName: ntdll.dll
OriginalFilename: ntdll.dll
ProductVersion: 5.2.3790.4789
FileVersion: 5.2.3790.4789 (srv03_sp2_gdr.101019-0340)
FileDescription: NT Layer DLL
LegalCopyright: c Microsoft Corporation. All rights reserved.

BR,
Alexei

=====