

minidump analysis

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.csharp/2005-12/msg00346.html>

- *From:* Droopy <droopytoonospam@xxxxxxxxxxxxx>
 - *Date:* 01 Dec 2005 15:56:24 GMT
-

Hi,

I wrote a C# application that seems to run quite well in our room.
Now, it is also running in another room and it crashes from time to time.
There is the following error in the LogEvent :

"Faulting application IPRRouting.exe, version 1.10.50.19217, faulting module kernel32.dll, version 5.1.2600.2180, fault address 0x000107f8."

A previous crash (on another PC) lead to following error :

"Faulting application IPRRouting.exe, version 1.10.50.19217, faulting module mswsock.dll, version 5.1.2600.2180, fault address 0x00002c61."

A window asking to send error to Microsoft appears and a minidump is generated.

I tried to analyse this minidump but it does not give me many clue about the problem. The only thing I see is "Stack buffer overflow" but is it really the source of the problem and if yes, what is the code that lead to this error ?

Here is the output from WinDbg :

Microsoft (R) Windows Debugger Version 6.1.0017.2
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\tmp\Tobo\WER5181.dir00\IPRRouting.exe.mdump]
User Mini Dump File: Only registers, stack and portions of memory are available

Windows XP Version 2600 (Service Pack 2) MP (2 procs) Free x86 compatible
Product: WinNt, suite: SingleUserTS
Debug session time: Thu Dec 01 15:30:40 2005
System Uptime: not available
Process Uptime: 3 days 3:35:33.000

minidump analysis

Symbol search path is: srv*c:

\symbols*<http://msdl.microsoft.com/download/symbols>

Executable search path is:

.....
.....

(1048.ad8): Stack buffer overflow – code c0000409 (!!! second chance !!!)

eax=06fb0000 ebx=7c910331 ecx=00001000 edx=7c90eb94 esi=00001ebc edi=00000000

eip=7c90eb94 esp=08e3ae4c ebp=08e3aeb0 iopl=0 nv up ei ng nz ac

po cy

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000297

ntdll!KiFastSystemCallRet:

7c90eb94 c3 ret

0:011> !analyse -v

No export analyse found

0:011> kd

ntdll!KiFastSystemCallRet

08e3ae48 00000000

08e3ae4c 7c90e9c0 ntdll!ZwWaitForSingleObject+0xc

08e3ae50 7c8025db kernel32!WaitForSingleObjectEx+0xa8

08e3ae54 00001ebc

08e3ae58 00000000

08e3ae5c 08e3ae80

08e3ae60 00000000

08e3ae64 00000001

08e3ae68 7c910331 ntdll!RtlGetLastWin32Error

08e3ae6c 00000014

08e3ae70 00000001

08e3ae74 00000000

08e3ae78 00000000

08e3ae7c 00000010

08e3ae80 4d2fa200

08e3ae84 ffffffff

08e3ae88 7ffdc000

08e3ae8c 7ffab000

08e3ae90 08e3ae80

08e3ae94 08e3b004

Here is the output for previous crash :

Microsoft (R) Windows Debugger Version 6.1.0017.2

Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [C:\tmp\Tobo\WERe643.dir00\IPRRouting.exe.mdump]

User Mini Dump File: Only registers, stack and portions of memory are available

Windows XP Version 2600 (Service Pack 2) MP (2 procs) Free x86 compatible

Product: WinNt, suite: SingleUserTS

minidump analysis

minidump analysis

```
Debug session time: Tue Nov 29 08:35:34 2005
System Uptime: not available
Process Uptime: 0 days 20:42:26.000
Symbol search path is: srv*c:
\symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
.....
.....
(814.830): Stack buffer overflow - code c0000409 (!!! second chance !!!)
eax=07be0000 ebx=7c910331 ecx=00001000 edx=7c90eb94 esi=000017a8 edi=
00000000
eip=7c90eb94 esp=0ba7b2d4 ebp=0ba7b338 iopl=0 nv up ei ng nz ac
po cy
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=
00000297
ntdll!KiFastSystemCallRet:
7c90eb94 c3 ret
0:054> !analyse -v
No export analyse found
0:054> kd
ntdll!KiFastSystemCallRet
0ba7b2d0 00000000
0ba7b2d4 7c90e9c0 ntdll!ZwWaitForSingleObject+0xc
0ba7b2d8 7c8025db kernel32!WaitForSingleObjectEx+0xa8
0ba7b2dc 000017a8
0ba7b2e0 00000000
0ba7b2e4 0ba7b308
0ba7b2e8 00000000
0ba7b2ec 00000001
0ba7b2f0 7c910331 ntdll!RtlGetLastWin32Error
0ba7b2f4 00000014
0ba7b2f8 00000001
0ba7b2fc 00000000
0ba7b300 00000000
0ba7b304 00000010
0ba7b308 4d2fa200
0ba7b30c ffffffff
0ba7b310 7ffde000
0ba7b314 7ff3d000
0ba7b318 0ba7b308
0ba7b31c 0ba7b48c
```

I also tried to load the minidump in VisualStudio 2003.

I got a first popup window with following text :

```
"IPRRouting.exe' does not contain debugging information. (No matching
binary found.) Click OK to debug anyway."
```

I pushed the 'OK' button.

minidump analysis

minidump analysis

Then I got another popup window with following text :

```
"Unhandled exception at 0x7c8107f8 in IPRRrouting.exe.mdmp: 0xC0000409: 0xc0000409."
```

I pushed the 'Break' button.

Then I got another popup window with following text :

```
"There is no source code available for the current location."
```

I pushed the 'OK' button.

I can only see the following lines in Call Stack window :

```
kernel32.dll!7c8107f8()  
kernel32.dll!7c8107f8()
```

With the previous crash, I saw these lines in Call Stack window :

```
msocket.dll!71a52c61()  
mscorwks.dll!791f92c9()  
mscorwks.dll!791f92c9()  
mscorwks.dll!791dc00f()  
mscorwks.dll!791dc017()  
mscorwks.dll!791dbfa4()  
mscorwks.dll!791dcf4f()  
mscorwks.dll!791da717()  
mscorwks.dll!791da434()  
mscorwks.dll!791d6e17()  
mscorwks.dll!791da320()  
mscorwks.dll!791da330()  
mscorwks.dll!791b517f()  
mscorwks.dll!791da58a()  
mscorwks.dll!791b517f()  
mscorwks.dll!791da5f6()  
mscorwks.dll!792e518c()  
mscorwks.dll!791c8c38()  
mscorwks.dll!792e525b()
```

Any help would be greatly appreciated, I don't know where to look for this problem !

Thanks in advance for your help,

Regards,

Droopy.

.

minidump analysis

- *Follow-Ups:*
 - ◆ *Re: minidump analysis*
 - ◇ *From:* Droopy
- Prev by Date: *Re: Newbie Question – Using Static (from VB.net) in C#*
- Next by Date: *Re: Starting a new process, which has the same security permissions and the parent.*
- Previous by thread: *Re: Newbie Question – Using Static (from VB.net) in C#*
- Next by thread: *Re: minidump analysis*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*