Crash location !

Posted by patra04 - 13 Aug 2010 - 21:09

Hello Folks,

I have a crash file which gives me the following information.

==========
An Exception Occurred:

Reason:
some.exe caused an EXCEPTION_ACCESS_VIOLATION in module some.dll at 001B:012C300B

Registers:
EAX=00910000 EBX=003425A0 ECX=012C7090 EDX=7C82860C ESI=012C7090
EDI=00000000 EBP=05CBF3C8 ESP=05CBF3B8 EIP=012C300B FLG=00010206
CS =001B DS =0023 SS =0023
ES =0023 FS =003B GS =0000

Call Stack:
001B:012C300B (0x00910048 0x009AE718 0x009AE6E0 0x009AE6EC) some.dll
001B:01A11027 (0x00910048 0x00000000 0x00000000 0x042CF0D8) one.dll
001B:0120834E (0x00910048 0x00941D58 0x00000000 0x00000000) two.dll
001B:0111DD9E (0x00000002 0x05CBFE34 0x05CBFA38 0x00000000) three.dll
001B:01113AC7 (0x05CBFA38 0x05CBFE34 0x05CBF9A4 0x00000001) four.dll
001B:011188BF (0x05CBFA38 0x00CBFE34 0x00000000 0x05CBFEC4) five.dll
001B:01104222 (0x05CBFA38 0x05CBFE34 0x00000000 0x05CBFEC4) six.dll
001B:0110B409 (0x074CA008 0x05CBFA38 0x05CBFE34 0x00000000) seven.dll

==========

I started winDBG and attached it to the instance of the faulty process on my local machine. I have all the correct PDBs and symbol path is set correctly.

The above crash file also stated that some.dll was loaded at 012C0000.

In my running instance I can see that some.dll is loaded at 017a0000.

Can I use the following command in my winDBG session to locate the crash location?

0:007> ln 017a300B

012C300B - 0x012C0000 = 300B = crash location?
For me it should it 017a0000 + 300B = 017a300B?

Or do I have to use

0:007> ln 017a200B

012C300B - 0x012C0000 -1000 = 200B?

Or am I wrong in my approach itself?

Thanks for your help and support.

Regards,
Rahul

==========

Re: Crash location !

Posted by Sclieu Yu - 29 Sep 2010 - 03:10

_____

Use the adplus.vbs script to monitor your executable and it will automatically generate a full dump when the proces has a 2nd chance exception (unhandled exception). There are parameters to the script, but it should look something like:

cscript adplus.vbs -crash -pn some.exe

When you open the dump file, you should see more information and line numbers if you have PDB files, which will help you determine exactly what's going on. Alternatively, you can attach to the process and do live debugging, but you'll need to be pretty savvy with the commands. They are all available on the online help.

==========