

Re: How to troubleshoot bugchecks on my own?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2008-01/msg00091.htm>

- *From:* "Ivan Brugiolo [MSFT]" <ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 8 Jan 2008 03:54:10 -0800
-

I still vote for a single bit error or other code/data alterations.

For example, a change from 85 -> a5 will give

```
a5 movs dword ptr [edi],dword ptr [esi]
```

that may cause an exception

To confirm, I would extract the exception record, from the stack, if it is saved, and if the machine did not switch stack as part of the bugcheck.

From that exception record and context, I would compare what was reported

as the trap-frame in the KiBugcheckData.

Depending on the type of dump (full or mini) and the type of operation that the crash-dump code has causes to physical-memory, the information you get may or may not be reliable.

--

--

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>

"Armin Zingler" <az.nospam@xxxxxxxxxxx> wrote in message news:OG8cmsdUIHA.4684@xxxxxxxxxxxxxxxxxxxxxxxx

Thanks a lot for your answer. I must admit that I do not completely understand everything. Sorry if I have to ask again:

Do you mean a virus /or/ a kernel hook? I don't have a resident virus scanner.

Only on demand. I don't dare to say it is impossible to have a virus on the system (spontaneously I'd say it is impossible because I'm the only user and I very well know what to do and what not), but after scanning the

Re: How to troubleshoot bugchecks on my own?

whole system, no virus/spyware/etc could be found.

Concerning memory faults: I ran memtest for so many hours meanwhile, that memory errors are close to impossible. At least what is commonly considered as being sufficient testing to exclude memory problems. The machine is also considered "primestable".

In general, I experienced many more BSODs since having a dual core CPU (after that reinstalled the system etc.). Often, if one has problems like these, you are blamed for doing this and that wrong. For simplification, you can believe me that all preconditions are met to have a working machine (starting with BIOS, power supply, etc...). In other words, I'd build the machine again exactly like it is now. I say this in advance because I now came to the point to focus /only/ on looking for software/driver problems. Looking in the event log, I had 24 BSOD since August. That's about once a week. Unacceptable. Before, I had no more than two in a year. That's why I finally want to find the cause of the problem, no matter how much time it costs.

What would you do now looking at the "!analyze" result? If I can not rely on the faulty statement, can I rely on the stack trace? Where is the problem? I still don't know what to do now. Sorry if I ask for more than what is possible.

Does it help if I say that I have another memory dump that also says:
FAILED_INSTRUCTION_ADDRESS: nt!IopXxxControlFile+37e8057f39a 85db test ebx,ebx

How can I use Windbg to narrow the problem down?

Thanks again

Armin

"Ivan Brugiolo [MSFT]" <ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx> schrieb

The instruction reported in the `!analyze` output may be the instruction that was mapped from the binary on disk in the machine where the analysis was performed, and, it may not necessarily be the instruction that was being executed at the time the bugcheck occurred.

For example, if you have some virus/kernel-hook, the code that is

Re: How to troubleshoot bugchecks on my own?

supposed to be there and the code that was there are not the same.

Likewise, a single bit memory error on the physical page containing the code being executed may have changed `test ebx, ebx` to something that was not a valid opcode.

--

--

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/cpyright.htm>

"Armin Zingler" <az.nospam@xxxxxxxxxxx> wrote in message news:OT%23PkaVUIHA.2000@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi, thx for your response. I read some pages meanwhile, but still don't know how to start. Well, I know that 0x8e is KERNEL_MODE_EXCEPTION_NOT_HANDLED. The Exception is 0xc000001d which means "illegal instruction". So, "test ebx,ebx" is illegal? Do I have to look for the assembler reference and/or lookup the opcode?

nt!IopXxxControlFile+37e
8057f39a 85db test ebx,ebx

Now, if I look at the stack and try to interpret it, I'm not even able to find out the driver or whatever causes the fault. The error is in module nt.dll. Nice, but what now?

You wrote "- to use verifier ON for suspicious driver". I didn't know what it means. I've searched and think that I'll be able to handle it, though, I don't know which driver might be suspicious.

I'd be glad if you could give me a hint.

Armin
PS: using the MSFT symbol server, I guess I do have the latest symbols.

"Volodymyr Shcherbyna"

Re: How to troubleshoot bugchecks on my own?

<v_scherbina@xxxxxxxxxxxxxxxx> schrieb

General recommendations are:

- to use verifier ON for suspicious driver
- to use WinDbg (or SoftIce) + latest symbols of windows binaries - to have much time to spend on analysys

--

Volodymyr

NG tips:

http://msmvps.com/blogs/v_scherbina/pages/microsoft-newsgroups-tips.aspx

"Armin Zingler"

<az.nospam@xxxxxxxx> wrote in message

<news:%23bZcZWSUIHA.3676@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"Armin Zingler"

<az.nospam@xxxxxxxx>
schrieb

I'd do the
work on my
own. But,
where to
start? Do
you have
a link about
the
"howto"?
Thanks!
(Though, I
appended
the output
below)

ok ok, googling
"troubleshoot bsod" does
reveal "some"
links... I'll read. Though, if
you still have helpful
information, I'm
still
instered.

Re: How to troubleshoot bugchecks on my own?

Armin