

Re: I need help to understand a double fault

Re: I need help to understand a double fault

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2009-07/msg00050.1>

- *From:* "Volodymyr Shcherbyna" <v_scherbina@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 3 Jul 2009 10:10:36 +0200
-

Try to show raw stack, and if you have several CPU's on machine, switch to different cpu stack (Alt + F9),

Sorry, Alt + 9

--

Volodymyr M. Shcherbyna, blog: <http://www.shcherbyna.com/>
(This posting is provided "AS IS" with no warranties, and confers no rights)

"Volodymyr Shcherbyna" <v_scherbina@xxxxxxxxxxxxxxxxxxxx> a écrit dans le message de news:eB4nNT7%23JHA.1340@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Try to show raw stack, and if you have several CPU's on machine, switch to different cpu stack (Alt + F9), as the second CPU stack might be also useful. The only thing which is obvious from your dump is that it is caused by machine check exception code which is calling HalHandleMcheck and it all ends up like this.

So, try to get raw stack, and put it here. Does this issue came out only at one particular 2k03 machine? Or it is repeatable on other machines?

--

Volodymyr M. Shcherbyna, blog: <http://www.shcherbyna.com/>
(This posting is provided "AS IS" with no warranties, and confers no rights)

"dLopesp" <dLopesp@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> a écrit dans le message de news:EBDBAB3B-3FB9-4483-8597-0BFB238DEF10@xxxxxxxxxxxxxxxxxxxx

Forgot to include kernel dump:

"dLopesp" wrote:

Hi,

Re: I need help to understand a double fault

unfortunately, there is something else wrong with my driver
(or with my
machine/board):

Please, take a look in the kernel dump analysis:

BugCheck 9C, {0, 808a07a0, b2000000, 1040080f}

PEB is paged out (Peb.Ldr = 7ffdc00c). Type ".hh dbgerr001" for details
PEB is paged out (Peb.Ldr = 7ffdc00c). Type ".hh dbgerr001" for details
Probably caused by : Unknown_Image (ANALYSIS_INCONCLUSIVE)

Followup: MachineOwner

0: kd> !analyze -v

```
*****
*
*
* Bugcheck Analysis
*
*
*
*****
```

MACHINE_CHECK_EXCEPTION (9c)

A fatal Machine Check Exception has occurred.

KeBugCheckEx parameters;

x86 Processors

If the processor has ONLY MCE feature available (For example Intel Pentium), the parameters are:

- 1 – Low 32 bits of P5_MC_TYPE MSR
- 2 – Address of MCA_EXCEPTION structure
- 3 – High 32 bits of P5_MC_ADDR MSR
- 4 – Low 32 bits of P5_MC_ADDR MSR

If the processor also has MCA feature available (For example Intel Pentium Pro), the parameters are:

- 1 – Bank number
- 2 – Address of MCA_EXCEPTION structure
- 3 – High 32 bits of MCI_STATUS MSR for the MCA bank that had the error
- 4 – Low 32 bits of MCI_STATUS MSR for the MCA bank that had the error

IA64 Processors

1 – Bugcheck Type

1 – MCA_ASSERT

2 – MCA_GET_STATEINFO

SAL returned an error for SAL_GET_STATEINFO while processing MCA.

3 – MCA_CLEAR_STATEINFO

SAL returned an error for SAL_CLEAR_STATEINFO while processing MCA.

Re: I need help to understand a double fault

4 – MCA_FATAL

FW reported a fatal MCA.

5 – MCA_NONFATAL

SAL reported a recoverable MCA and we don't support currently support recovery or SAL generated an MCA and then couldn't produce an error record.

0xB – INIT_ASSERT

0xC – INIT_GET_STATEINFO

SAL returned an error for SAL_GET_STATEINFO while processing INIT event.

0xD – INIT_CLEAR_STATEINFO

SAL returned an error for SAL_CLEAR_STATEINFO while processing INIT event.

0xE – INIT_FATAL

Not used.

2 – Address of log

3 – Size of log

4 – Error code in the case of x_GET_STATEINFO or x_CLEAR_STATEINFO

AMD64 Processors

1 – Bank number

2 – Address of MCA_EXCEPTION structure

3 – High 32 bits of MCi_STATUS MSR for the MCA bank that had the error

4 – Low 32 bits of MCi_STATUS MSR for the MCA bank that had the error

Arguments:

Arg1: 00000000

Arg2: 808a07a0

Arg3: b2000000

Arg4: 1040080f

Debugging Details:

NOTE: This is a hardware error. This error was reported by the CPU via Interrupt 18. This analysis will provide more information about the specific error. Please contact the manufacturer for additional information about this error and troubleshooting assistance.

This error is documented in the following publication:

– IA-32 Intel(r) Architecture Software Developer's Manual
Volume 3: System Programming Guide

Bit Mask:

MA Model Specific MCA

O ID Other Information Error Code Error Code

VV SDP _____|_____ _____|_____ _____|_____

AEUECRC| | | |

LRCNVVC| | | |

^^^^^^| | | |

Re: I need help to understand a double fault

LAST_CONTROL_TRANSFER: from 80a84154 to 8087c480

STACK_TEXT:

808a0770 80a84154 0000009c 00000000 808a07a0 nt!KeBugCheckEx+0x1b
808a08a4 80a7b86f 80042000 00000000 00000000
hal!HalpMcaExceptionHandler+0x11e
808a08a4 10216177 80042000 00000000 00000000
hal!HalpMcaExceptionHandlerWrapper+0x77
WARNING: Frame IP not in any known module. Following frames may be
wrong.
0770fd80 00000000 00000000 00000000 00000000 0x10216177

STACK_COMMAND: kb

SYMBOL_NAME: ANALYSIS_INCONCLUSIVE

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: Unknown_Module

IMAGE_NAME: Unknown_Image

DEBUG_FLR_IMAGE_TIMESTAMP: 0

FAILURE_BUCKET_ID:

0x9C_GenuineIntel_VRF_ANALYSIS_INCONCLUSIVE

BUCKET_ID: 0x9C_GenuineIntel_VRF_ANALYSIS_INCONCLUSIVE

Followup: MachineOwner

Could anyone take help me to understand this? After
googling about this
error code I saw that this error might be related to
overclocking (which is
not the case) or bad motherboards.

I'm kind of lost here.
Thanks for any help.
Regards,
Douglas

"dLopesp" wrote:

> Hi Volodymyr,
>

Re: I need help to understand a double fault

> I added a check to the code that was causing the BSOD.
Now my driver > will
> only cancel the request if it is still in one of my driver's
queues > (meaning
> the request is still in the driver since I don't remove
requests from > queue
> while processing them). Otherwise my driver will do
nothing. This is > what it
> looks like:
>
> EvtCancelFunction()
> {
> ...
>
> if (WdfRequestGetIoQueue(request))
> {
> WdfRequestSetInformation(request, info);
> WdfRequestUnmarkCancelable(request);
>
>
> WdfRequestCompleteWithPriorityBoost(request,status,IO_NO_INCREMENT);
> }
>
> // end of EvtCancelFunction()
> }
>
> The good news is that with this modification the BSOD
has not > happened.
> The bad news is that my test application is stucked. It
looks like the
> request that was not cancelled is stucked in my driver
preventing my
> application to close successfully.
>
> Can anyone propose a more elegant (and efficient)
solution?
>
> Thanks for your colaboration.
> Best regards,
> Douglas
>
> "Volodymyr Shcherbyna" wrote:
>
>> Hello,
>>
>> I am not sure I understand what exactly is going on in
your code. As >> the
>> only thing I see is a small snippet of code and a stack
trace :). >> However,
>> as I saw it, I reminded this case:
>>

Re: I need help to understand a double fault

<http://blogs.msdn.com/doronh/archive/2008/06/29/how-do-i-cancel-an-irp-that-another-th>
>>
>>> Is there a possibility of concurrency? Something like
the cancel >>> was
>>> invoked
>>> and just after that my driver completed the request then
I got >>> back to
>>> process the cancel request.
>>
>> Yep, it can happen like this as well. But, I need to see
more code >> to
>> answer. Or, at least, explain how do you process IRP and
under which
>> condition you decide to cancel it.
>>
>> -- >> Volodymyr M. Shcherbyna, blog:
<http://www.shcherbyna.com/>
>> (This posting is provided "AS IS" with no warranties,
and confers no
>> rights)
>>
>> "dLopesp" <dLopesp@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
a écrit dans le >> message de
>>
<news:34881C9E-B7FB-46E8-91B5-B865B6115B7E@xxxxxxxxxxxxxxxxxxx>
>>> Thanks for your time Mr. Volodymyr.
>>>
>>> I ran my driver compiled in a Windows Server 2003
Checked >>> environment for
>>> more than 22 hours. When I was about to stop my test
scenario I >>> got the
>>> following BSOD:
>>>
>>> BugCheck 8E, {c0000005, ba949ac9, b82a99b4, 0}
>>>
>>> Page 75bb4 not present in the dump file. Type ".hh
dbgerr004" for >>> details
>>> Page 71c76 not present in the dump file. Type ".hh
dbgerr004" for >>> details
>>> PEB is paged out (Peb.Ldr = 7ffd400c). Type ".hh
dbgerr001" for >>> details
>>> PEB is paged out (Peb.Ldr = 7ffd400c). Type ".hh
dbgerr001" for >>> details
>>> Probably caused by : mydriver.sys (>>>
mydriver!WdfRequestSetInformation+1a)
>>>
>>> Followup: MachineOwner
>>> -----
>>>
>>> 1: kd> !analyze -v
>>>

Re: I need help to understand a double fault

Re: I need help to understand a double fault

```
*****
>>> *
>>> *
>>> * Bugcheck Analysis
>>> *
>>> *
>>> *
>>>
*****
>>>
>>> KERNEL_MODE_EXCEPTION_NOT_HANDLED
(8e)
>>> This is a very common bugcheck. Usually the
exception address >>> pinpoints
>>> the driver/function that caused the problem. Always
note this >>> address
>>> as well as the link date of the driver/image that
contains this >>> address.
>>> Some common problems are exception code
0x80000003. This means a >>> hard
>>> coded breakpoint or assertion was hit, but this system
was booted
>>> /NODEBUG. This is not supposed to happen as
developers should >>> never have
>>> hardcoded breakpoints in retail code, but ...
>>> If this happens, make sure a debugger gets connected,
and the
>>> system is booted /DEBUG. This will let us see why
this breakpoint >>> is
>>> happening.
>>> Arguments:
>>> Arg1: c0000005, The exception code that was not
handled
>>> Arg2: ba949ac9, The address that the exception
occurred at
>>> Arg3: b82a99b4, Trap Frame
>>> Arg4: 00000000
>>>
>>> Debugging Details:
>>> -----
>>>
>>> Page 75bb4 not present in the dump file. Type ".hh
dbgerr004" for >>> details
>>> Page 71c76 not present in the dump file. Type ".hh
dbgerr004" for >>> details
>>> PEB is paged out (Peb.Ldr = 7ffd400c). Type ".hh
dbgerr001" for >>> details
>>> PEB is paged out (Peb.Ldr = 7ffd400c). Type ".hh
dbgerr001" for >>> details
>>>
>>> EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - A
```

Re: I need help to understand a double fault

```
instru o no "0x%08lx" >>> fez refer
>>> ncia mem ria no "0x%08lx". A mem ria n o p de ser
"%s".
>>>
>>> FAULTING_IP:
>>> wdf01000!FxRequest::SetInformation+69
>>> ba949ac9 89481c mov dword ptr [eax+1Ch],ecx
>>>
>>> TRAP_FRAME: b82a99b4 -- (.trap
0xfffffff82a99b4)
>>> ErrCode = 00000002
>>> eax=00000000 ebx=89818730 ecx=00000000
edx=89818730 esi=886e8d00
>>> edi=89818678
>>> eip=ba949ac9 esp=b82a9a28 ebp=b82a9a30 iopl=0 nv
up ei pl >>> zr na pe
>>> nc
>>> cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000
>>> efl=00010246
>>> wdf01000!FxRequest::SetInformation+0x69:
>>> ba949ac9 89481c mov dword ptr [eax+1Ch],ecx
>>> ds:0023:0000001c=????????
>>> Resetting default scope
>>>
>>> DEFAULT_BUCKET_ID:
INTEL_CPU_MICROCODE_ZERO
>>>
>>> BUGCHECK_STR: 0x8E
>>>
>>> PROCESS_NAME: testaplication.exe
>>>
>>> CURRENT_IRQL: 0
>>>
>>> LAST_CONTROL_TRANSFER: from 8085bba7 to
8087c480
>>>
>>> STACK_TEXT:
>>> b82a9580 8085bba7 0000000e c0000005 ba949ac9
nt!KeBugCheckEx+0x1b
>>> b82a9944 808346b4 b82a9960 00000000 b82a99b4 >
>> nt!KiDispatchException+0x3a2
>>> b82a99ac 80834668 b82a9a30 ba949ac9 badb0d00
>>> nt!CommonDispatchException+0x4a
>>> b82a99cc 80a801ae 00000000 8980b800 00000202 >
>> nt!Kei386EoiHelper+0x186
>>> b82a9a30 ba9358ac 00000000 00000000 886e8d54
>>> hal!HalpDispatchSoftwareInterrupt+0x5e
>>> b82a9a48 ba8eb2ca 886e8d00 779172f8 00000000
>>> wdf01000!imp_WdfRequestSetInformation+0x7c
>>> b82a9a5c ba8f4c47 779172f8 00000000 00000000
>>> mydriver!WdfRequestSetInformation+0x1a
```

Re: I need help to understand a double fault

```
>>> [c:\winddk\6001.18001\inc\wdf\kmdf\1.7\wdfrequest.h
@ 1277]
>>> b82a9a8c ba95b45b 779172f8 8980b7f0 886e8d00
>>> mydriver!MyDriverEvtRequestCancel+0x157
[d:\myDriverUtil.c @ 1575]
>>> b82a9aa4 ba95d573 00000000 779172f8 8980b7f0
>>>
wdf01000!FxRequestCancelAndCompletion::InvokeCancel+0x2f
>>> b82a9acc ba95ed95 b82a9af4 00000000 8980b7f0
>>>
wdf01000!FxIoQueue::ProcessCancelledRequests+0x15b
>>> b82a9aec ba960929 8980b700 8980b7f0 885f4cb0
>>> wdf01000!FxIoQueue::DispatchEvents+0x2c6
>>> b82a9b08 ba961b4b 885f4cb0 ba986188 89818678
>>>
wdf01000!FxIoQueue::QueueRequestFromForward+0x1e3
>>> b82a9b2c ba943972 8980c640 885f4cb0 767f39b8
>>> wdf01000!FxPkgIo::EnqueueRequest+0x21d
>>> b82a9b40 ba8f4eea 885f4cb0 8980c640 77a0b348
>>> wdf01000!imp_WdfDeviceEnqueueRequest+0x49
>>> b82a9b54 ba8f4f38 767f39b8 77a0b348 898110d8
>>> mydriver!WdfDeviceEnqueueRequest+0x1a
>>> [c:\winddk\6001.18001\inc\wdf\kmdf\1.7\wdfdevice.h
@ 3181]
>>> b82a9b68 ba96172f 767f39b8 77a0b348 8980bc10
>>> mydriver!MyDriverEvtIoInCallerContext+0x38
[d:\myDriverUtil.c @ >>> 1772]
>>> b82a9b90 ba940fbc 898c9e60 8980bc10 0000000e
>>> wdf01000!FxPkgIo::Dispatch+0x249
>>> b82a9ba8 ba8f50ca 8980c640 767f39b8 898c9e60
>>>
wdf01000!imp_WdfDeviceWdmDispatchPreprocessedIrp+0xf1
>>> b82a9bbc ba8f509b 767f39b8 898c9e60 b82a9c14
>>>
mydriver!WdfDeviceWdmDispatchPreprocessedIrp+0x1a
>>> [c:\winddk\6001.18001\inc\wdf\kmdf\1.7\wdfdevice.h
@ 1480]
>>> b82a9be8 ba94ff4b 767f39b8 898c9e60 80a7ff00
>>> mydriver!MyDriverEvtWdmIrpPreprocess+0x13b
[d:\myDriverUtil.c @ >>> 1866]
>>> b82a9c08 ba950618 898c9e60 b82a9c44 809d657d
>>> wdf01000!FxDevice::PreprocessIrp+0x7b
>>> b82a9c14 809d657d 8980bc10 898c9e60 898c9e60
>>> wdf01000!FxDevice::Dispatch+0x32
>>> b82a9c44 80859d70 8092b50f b82a9c64 8092b50f >>
> nt!IovCallDriver+0x112
>>> b82a9c50 8092b50f 898c9ef4 8831fd20 898c9e60
nt!IofCallDriver+0x13
>>> b82a9c64 8092b444 8980bc10 898c9e60 8831fd20
>>> nt!IopSynchronousServiceTail+0x10b
>>> b82a9d00 8092b564 00002778 00000000 00000000 >
```

Re: I need help to understand a double fault

```
>> nt!IopXxxControlFile+0x60f
>>> b82a9d34 80833bdf 00002778 00000000 00000000 >
>> nt!NtDeviceIoControlFile+0x2a
>>> b82a9d34 7c8285ec 00002778 00000000 00000000 >
>> nt!KiFastCallEntry+0xfc
>>> WARNING: Frame IP not in any known module.
Following frames may be >>> wrong.
>>> 0012fa0c 00000000 00000000 00000000 00000000
0x7c8285ec
>>>
>>>
>>> STACK_COMMAND: kb
>>>
>>> FOLLOWUP_IP:
>>> mydriver!WdfRequestSetInformation+1a
>>> [c:\winddk\6001.18001\inc\wdf\kmdf\1.7\wdfrequest.h
@ 1277]
>>> ba8eb2ca 5d pop ebp
>>>
>>> FAULTING_SOURCE_CODE:
>>> 1273: ULONG_PTR Information
>>> 1274: )
>>> 1275: {
>>> 1276: ((PFN_WDFREQUESTSETINFORMATION)
WdfFunctions[WdfRequestSetInformationTableIndex])(WdfDriverGlobals,
>>> Request,
>>> Information);
>>>> 1277: }
>>> 1278:
>>> 1279: //
>>> 1280: // WDF Function: WdfRequestGetInformation
>>> 1281: //
>>> 1282: typedef
>>>
>>>
>>> SYMBOL_STACK_INDEX: 6
>>>
>>> SYMBOL_NAME:
mydriver!WdfRequestSetInformation+1a
>>>
>>> FOLLOWUP_NAME: MachineOwner
>>>
>>> MODULE_NAME: mydriver
>>>
>>> IMAGE_NAME: mydriver.sys
>>>
>>> DEBUG_FLR_IMAGE_TIMESTAMP: 4a4b58a8
>>>
>>> FAILURE_BUCKET_ID:
0x8E_VRF_mydriver!WdfRequestSetInformation+1a
```

Re: I need help to understand a double fault

>>>
>>> BUCKET_ID:
0x8E_VRF_mydriver!WdfRequestSetInformation+1a
>>>
>>> Followup: MachineOwner
>>> -----
>>>
>>> Unfortunately, after analysing the dump, I was unable
to >>> understand what
>>> caused that BSOD. This is the code on my
EvtRequestCancel routine:
>>>
>>> WdfRequestSetInformation(request, info);
>>> WdfRequestUnmarkCancelable(request);
>>>
>>> WdfRequestCompleteWithPriorityBoost(request,status,IO_NO_INCREMENT);
>>>
>>> Is there a possibility of concurrency? Something like
the cancel >>> was
>>> invoked
>>> and just after that my driver completed the request then
I got >>> back to
>>> process the cancel request.
>>>
>>> Thanks for all your help.
>>> Regards,
>>> Douglas
>>>
>>>
>>> "Volodymyr Shcherbyna" wrote:
>>>
>>>> "dLopesp"
<dLopesp@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message
>>>>
news:B8E78365-7BB8-410F-A2CE-E3BB8FCC147C@xxxxxxxxxxxxxxxxxxxx
>>>>
>>>>> Should it be a problem if I compile my driver on
Windows Vista >>>>> build
>>>>> environment to run it on Windows 2003?
>>>>>
>>>>> Theoretically could be, but practically ... If you
would compile >>>>> driver
>>>>> for
>>>>> Vista and compiler would put unknown kernel
routine which does >>>>> not exist
>>>>> in
>>>>> 2003 Server kernel, you driver simply would not load
(i.e., >>>>> DriverEntry
>>>>> not

Re: I need help to understand a double fault

>>> called, and error is written into Even Log).
>>>
>>>> Scott, this problem only happens no my windows
2003 machine. >>>> The same
>>>> driver
>>>> is running on windows vista (both 32 and 64bit
version) with no
>>>> problem.
>>>>
>>>> As many suggested here, setup verifier and make
tests. It should >>>> give you
>>>> enough information about the problem. If I would
met such >>>> problem, I
>>>> would
>>>> setup verifier, and if this would not help, I would
setup >>>> verifier and
>>>> Windows 2003 Checked/Debug build. It does not
take much time, 1 >>>> hour to
>>>> setup machine and you, hopefully, will have more
information.

_____ Information from ESET Smart Security, version of virus
signature database 4210 (20090702) _____

The message was checked by ESET Smart Security.

<http://www.eset.com>

_____ Information from ESET Smart Security, version of virus signature database 4211
(20090702) _____

The message was checked by ESET Smart Security.

<http://www.eset.com>

_____ Information from ESET Smart Security, version of virus signature database 4211 (20090702)

The message was checked by ESET Smart Security.

Re: I need help to understand a double fault

Re: I need help to understand a double fault

<http://www.eset.com>