

Re: Illegal instruction – code c000001d (!!! second chance !!!)

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2007-12/msg00506.html>

- *From:* vijayaraju.k@xxxxxxxxxx
 - *Date:* Thu, 27 Dec 2007 12:54:18 -0800 (PST)
-

On Dec 28, 1:29 am, "Ivan Brugiolo [MSFT]"
<ivanb...@xxxxxxxxxxxxxxxxxxxxxxxx> wrote:

I guess you need NOT to leave anything (IRPs, WorkItems, DPCs, etc) outstanding before unloading.
As far as the check-vs-free, my take is that it is timing.
Maybe the outstanding IRP below completes before you get unloaded, because the machine/driver is slower.
Or, you get lucky to get reloaded to the same address, and, you never notice the problem.

--

--

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>

<vijayaraj...@xxxxxxxxxx> wrote in message

news:138f0ddf-ab81-4eab-b419-9003177f8ea0@xx

On Dec 28, 1:01 am, "Ivan Brugiolo [MSFT]"

<ivanb...@xxxxxxxxxxxxxxxxxxxxxxxx> wrote:

It's possible that the routine that was passed to the WFD framework is invalid, because the driver was unloaded and then loaded to a different address.
Or, the address of the routine (because of unload-and-reuse) now points to something completely different, such as a mapped-view of a file, or a piece of pool.

Re: Illegal instruction – code c000001d (!!! second chance !!!)

--

--

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>

<vijayaraj...@xxxxxxxxxx> wrote in message

news:fe0f19e8-376a-4c41-bce1-87c848c87137@xx

Hi Experts,

I have developed a USB-UART Single KMDF driver for TUSB3410 Device. The device appears as Virtual Com Port in Device manager. I have both the Build versions for this driver Checked and Release. When I loaded the Checked Build versions of the driver Everything seems to be good and device works as expected. Device Open,close,init and Un-init everything works very well including File transfers in Hyper terminal, invidual Reads and Writes. But my problem is when I try to load the Free Build version of the Driver the system crashes with following last line of Error: Illegal instruction – code c000001d (!!! second chance !!!) f88d4dde 8d ???

and the crash dump for this driver is as follows:

*

Re: Illegal instruction – code c000001d (!!! second chance !!!)

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

Use !analyze -v to get detailed debugging information.

BugCheck FC, {f88d4ddc, 2eed163, f88d4d64, 0}

Probably caused by : Wdf01000.sys (Wdf01000!
FxRequestBase::CompleteSubmitted+89)

Followup: MachineOwner

```
kd> !analyze -v
*****
*
*
* Bugcheck
Analysis *
*
*
*****
```

ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY
(fc)
An attempt was made to execute non-executable memory.
The guilty
driver
is on the stack trace (and is typically the current instruction
pointer).
When possible, the guilty driver's name (Unicode string) is
printed on
the bugcheck screen and saved in KiBugCheckDriver.
Arguments:
Arg1: f88d4ddc, Virtual address for the attempted execute.

Re: Illegal instruction – code c000001d (!!! second chance !!!)

Arg2: 02eed163, PTE contents.
Arg3: f88d4d64, (reserved)
Arg4: 00000000, (reserved)

Debugging Details:

DEFAULT_BUCKET_ID: DRIVER_FAULT

BUGCHECK_STR: 0xFC

PROCESS_NAME: System

TRAP_FRAME: f88d4d64 -- (.trap 0xfffffff88d4d64)
ErrCode = 00000011
eax=c0000016 ebx=00000000 ecx=00000000 edx=00000002
esi=7dfe1fe8
edi=8233b8fc
eip=f88d4ddc esp=f88d4dd8 ebp=824b76d0 iopl=0 nv up ei
pl zr
na pe nc
cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000
efl=00010246
f88d4ddc 044e add al,4Eh
Resetting default scope

LAST_CONTROL_TRANSFER: from 8051c0d3 to
804f8aef

STACK_TEXT:
f88d4cec 8051c0d3 000000fc f88d4ddc 02eed163
nt!KeBugCheckEx+0x1b
f88d4d4c 8053f90c 00000008 f88d4ddc 00000000
nt!MmAccessFault+0x8e7
f88d4d4c f88d4ddc 00000008 f88d4ddc 00000000
nt!KiTrap0E+0xcc
WARNING: Frame IP not in any known module. Following

Re: Illegal instruction – code c000001d (!!! second chance !!!)

frames may be
wrong.
f88d4ddc aa030245 7db48928 7db3f600 8233b8fc
0xf88d4ddc
f88d4e04 aa0075d3 827aa51b 824c09f8 00000000
Wdf01000!
FxRequestBase::CompleteSubmitted+0x89
f88d4e20 aa00768d 014b76d0 8236e928 f88d4e4c
Wdf01000!
FxIoTarget::RequestCompletionRoutine+0x195
f88d4e30 804ef5ed 00000000 827aa460 824b76d0
Wdf01000!
FxIoTarget::_RequestCompletionRoutine+0x35
f88d4e4c 804f054c 00000000 827aa460 8236e928
nt!IopUnloadSafeCompletion
+0x1d
f88d4e7c f7f51ee5 827aa460 81c0fe10 82750028
nt!IopfCompleteRequest
+0xa2
f88d4ee4 f7f52b57 81fee4d8 00000000 827507d8
USBPORT!
USBPORT_CompleteTransfer+0x373
f88d4f14 f7f53754 026e6f44 827500e0 827500e0
USBPORT!
USBPORT_DoneTransfer+0x137
f88d4f4c f7f54f6a 82750028 80541ac8 82750230
USBPORT!
USBPORT_FlushDoneTransferList+0x16c
f88d4f78 f7f62fb0 82750028 80541ac8 82750028
USBPORT!USBPORT_DpcWorker
+0x224
f88d4fb4 f7f63128 82750028 00000001 82489008
USBPORT!
USBPORT_IsrDpcWorker+0x37e
f88d4fd0 80540f7d 8275064c 6b755044 00000000
USBPORT!USBPORT_IsrDpc
+0x166
f88d4ff4 80540c4a f8930c18 00000000 00000000
nt!KiRetireDpcList+0x46
f88d4ff8 f8930c18 00000000 00000000 00000000
nt!KiDispatchInterrupt
+0x2a
80540c4a 00000000 00000009 bb835675 00000128
0xf8930c18

STACK_COMMAND: kb

Re: Illegal instruction – code c000001d (!!! second chance !!!)

FOLLOWUP_IP:

Wdf01000!FxRequestBase::CompleteSubmitted+89

aa030245 eb0c jmp Wdf01000!

FxRequestBase::CompleteSubmitted+0x97 (aa030253)

SYMBOL_STACK_INDEX: 4

SYMBOL_NAME:

Wdf01000!FxRequestBase::CompleteSubmitted+89

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: Wdf01000

IMAGE_NAME: Wdf01000.sys

DEBUG_FLR_IMAGE_TIMESTAMP: 4549b23a

FAILURE_BUCKET_ID:

0xFC_Wdf01000!FxRequestBase::CompleteSubmitted+89

BUCKET_ID:

0xFC_Wdf01000!FxRequestBase::CompleteSubmitted+89

Followup: MachineOwner

Can anybody help me in this regard? I don't know How to debug further and what to do next as the error is not in my driver? Please somebody help me to get rid of this problem, It is very urgent

Re: Illegal instruction – code c000001d (!!! second chance !!!)

for me.
Your valuable suggestions are always appreciable.
Thanks in advance.

~Vijji– Hide quoted text –

– Show quoted text –

Hi Ivan,
Thanks for the Immediate reply.
You are absolutely correct. My driver gets reloaded because, I have
firmware download in my driver hence I need to Recycle/Reload the
driver after downloading the firmware by using
"WdfUsbTargetDeviceCyclePortSynchronously".

So what do you think I can do to fix this issue? Why is it effects
only in Free Build of the driver?
Thnaks in advance.

~Vijji– Hide quoted text –

– Show quoted text –

Hi Ivan,
Thats verymuch reasonable. I understood about Check–VS–Free build
matter clearly now.
But I din't get you on these following lines
"I guess you need NOT to leave anything (IRPs, WorkItems, DPCs, etc)
outstanding before unloading."
What do you mean by that? Something needs to be changed in driver?
Usually at the time of Firmware download and Power Policy Setting I am
calling the "WdfUsbTargetDeviceCyclePortSynchronously" routine This
routine causes my driver gets unloaded by calling surprise removal and
then restart/reenumerate the device by calling DriverEntry routine.
When it calls surprise remove routine consequently Its also calls
ReleaseHardware routine to remove everything that was prepared/started
at the time of PrepareHardware. I think nothing remains in the
driver,everything will be re–created and re–assigned I hope.
Can you please help in understanding and resolving this Issue?
How can you solve this problem? Suggest me to solve this problem.

~Vijji

Re: Illegal instruction – code c000001d (!!! second chance !!!)