

Re: Standby–Sleep Problem

Source:

<http://www.tech–archive.net/Archive/Development/microsoft.public.development.device.drivers/2007–05/msg00488.1>

- *From:* "Thomas F. Divine" <tdivine@NOpcausaSPAM>
 - *Date:* Tue, 22 May 2007 11:34:44 –0400
-

James,

Please don't post the same message three times. One time will do nicely.

Certainly the steps that you took should not cause a crash. That would be stupid.

If your driver does not explicitly show up in the crash dump, then it does not mean that the crash is not your driver's fault. You could be passing faulty data to some other driver or your driver could have some missing entry points.

You must use a debugger to study this problem. If you cannot attach a debugger, then you will not be successful in developing your driver. Analyzing crash dumps is NOT a substitute for having a debugger.

Attach a debugger and set breakpoints at key functions – especially those associated with unloading the device.

Read the DDK documentation and the sample. The DDK documentation should identify all of the required entry points that you must support. If you omit some, then that could be a problem.

Good luck,

Thomas F. Divine

"James" <James.Smith000@xxxxxxxxxx> wrote in message
<news:1179846735.233943.177790@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi All,

Im implementing a USB driver based on usbsamp sample provided in KMDF.
I have implemented D0Entry and D0Exit for handling PnP and Power Management.

I performed following sequence of steps:

- 1) Installed the driver.
- 2) Made the system to enter into Standby / Sleep state.
- 3) Un–Plugged the device.

Re: Standby–Sleep Problem

4) Pressed the power button to resume back.

After resume i see the crash and here is the log of it. I dont see any calls from my driver.

I would like to know if this is the expected behaviour.

or

Do i need to handle additional power settings to avoid crash.

All your suggestions are appreciable.

Thank You.

Regards,
James

*** Fatal System Error: 0x0000007e
(0xC0000005,0xF8661371,0xF89489B0,0xF89486AC)

Break instruction exception – code 80000003 (first chance)

A fatal system error has occurred.
Debugger entered on first try; Bugcheck callbacks have not been invoked.

A fatal system error has occurred.

Connected to Windows XP 2600 x86 compatible target, ptr64 FALSE
Loading Kernel Symbols

.....
Loading User Symbols

Loading unloaded module list

.....

*
*
* Bugcheck
Analysis *
*
*

Use !analyze -v to get detailed debugging information.

BugCheck 7E, {c0000005, f8661371, f89489b0, f89486ac}

Probably caused by : Wdf01000.sys (Wdf01000!FxPkgFdo::RaiseDevicePower

Re: Standby-Sleep Problem

+50)

Followup: MachineOwner

nt!RtlpBreakWithStatusInstruction:

80526da8 cc int 3

kd> !analyze -v

```

*****
*
*
* Bugcheck
Analysis *
*
*
*****

```

SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)

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.

Arguments:

- Arg1: c0000005, The exception code that was not handled
- Arg2: f8661371, The address that the exception occurred at
- Arg3: f89489b0, Exception Record Address
- Arg4: f89486ac, Context Record Address

Debugging Details:

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at "0x%08lx" referenced memory at "0x%08lx". The memory could not be "%s".

FAULTING_IP:

usbhub!USBH_SetPowerD0+d3
f8661371 8908 mov dword ptr [eax],ecx

EXCEPTION_RECORD: f89489b0 -- (.exr 0xfffffffff89489b0)
ExceptionAddress: f8661371 (usbhub!USBH_SetPowerD0+0x000000d3)
ExceptionCode: c0000005 (Access violation)
ExceptionFlags: 00000000
NumberParameters: 2
Parameter[0]: 00000001
Parameter[1]: 00000107
Attempt to write to address 00000107

CONTEXT: f89486ac -- (.cxr 0xfffffffff89486ac)
eax=00000107 ebx=82721c7c ecx=825fdbbc edx=825fdbbc esi=825fd948

Re: Standby-Sleep Problem

edi=81e92a28
eip=f8661371 esp=f8948a78 ebp=f8948a90 iopl=0 nv up ei pl nz
ac po cy
cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000
efl=00010213
usbhub!USBH_SetPowerD0+0xd3:
f8661371 8908 mov dword ptr [eax],ecx ds:
0023:00000107=????????
Resetting default scope

PROCESS_NAME: System

ERROR_CODE: (NTSTATUS) 0xc0000005 – The instruction at "0x%08lx"
referenced memory at "0x%08lx". The memory could not be "%s".

WRITE_ADDRESS: 00000107

BUGCHECK_STR: 0x7E

DEFAULT_BUCKET_ID: NULL_CLASS_PTR_DEREFERENCE

LAST_CONTROL_TRANSFER: from f86614b2 to f8661371

STACK_TEXT:

f8948a90 f86614b2 81e54008 00000100 81e92a28 usbhub!
USBH_SetPowerD0+0xd3
f8948aac f8661727 81e92a28 81e54008 81e54008 usbhub!USBH_PdoSetPower
+0x80
f8948acc f865997b 81e540c0 81e54008 00000002 usbhub!USBH_PdoPower
+0x201
f8948aec f86571d8 81e92a28 81e54008 f8948b20 usbhub!USBH_PdoDispatch
+0x83
f8948afc 804eddf9 81e92970 81e54008 81e540c0 usbhub!USBH_HubDispatch
+0x48
f8948b0c 8052222b 81e540c0 81e54008 00000000 nt!IopfCallDriver+0x31
f8948b20 80522745 81e540c0 81e54008 81e540dc nt!PopPresentIrp+0x57
f8948b40 aa4a069c 81e92970 81e92b58 81e83128 nt!PoCallDriver+0x195
f8948b60 aa4a0763 f8948ba0 aa4b3790 81e540e4 Wdf01000!
FxPkgFdo::RaiseDevicePower+0x50
f8948b74 aa4a0798 81e540e4 f8948ba4 aa4940d6 Wdf01000!
FxPkgFdo::DispatchDeviceSetPower+0xb6
f8948b80 aa4940d6 81e83128 f8948ba0 00000000 Wdf01000!
FxPkgFdo::_DispatchSetPower+0x23
f8948ba4 aa47dd9a 81e54008 f8948bcc aa47df9f Wdf01000!
FxPkgPnp::Dispatch+0x26e
f8948bb0 aa47df9f 81e86420 81e54008 80558ce8 Wdf01000!
FxDevice::Dispatch+0x7f
f8948bcc 804eddf9 81e86420 81e54008 81e540e4 Wdf01000!
FxDevice::DispatchWithLock+0x5d
f8948bdc 8052222b 81e540e4 81e54008 00000000 nt!IopfCallDriver+0x31
f8948bf0 80522745 81e540e4 81e54008 81e54108 nt!PopPresentIrp+0x57

Re: Standby-Sleep Problem

f8948c10 805228b5 81e86420 81e864f0 00000000 nt!PoCallDriver+0x195
f8948c2c aa49f43f 81e86420 00000002 00000001 nt!PoRequestPowerIrp
+0x129
f8948c68 aa49fb06 00000001 00000001 f8948cf0 Wdf01000!
FxPkgPnp::PowerPolicySendDevicePowerRequest+0x4d
f8948c78 aa49e592 81e83128 aa4b49c8 81e83128 Wdf01000!
FxPkgPnp::PowerPolSystemWakeDeviceWakeTriggeredS0+0x11
f8948cf0 aa49f07d 0000052d 81e8329c 81e83128 Wdf01000!
FxPkgPnp::PowerPolicyEnterNewState+0x169
f8948d18 aa49f394 f8948d48 806d06e0 81e83290 Wdf01000!
FxPkgPnp::PowerPolicyProcessEventInner+0x20b
f8948d2c aa49ff34 81e83128 f8948d48 81e85b58 Wdf01000!
FxPkgPnp::_PowerPolicyProcessEventInner+0x26
f8948d58 aa49ffdc f8948d74 8056abd5 81e86420 Wdf01000!
FxEventQueue::EventQueueWorker+0x47
f8948d60 8056abd5 81e86420 81e83290 8055a1fc Wdf01000!
FxThreadedEventQueue::_WorkItemCallback+0xd
f8948d74 80533dd0 81e85b58 00000000 82bc8640 nt!IopProcessWorkItem
+0x13
f8948dac 805c4a28 81e85b58 00000000 00000000 nt!ExpWorkerThread+0x100
f8948ddc 80540fa2 80533cd0 00000001 00000000 nt!PspSystemThreadStartup
+0x34
00000000 00000000 00000000 00000000 00000000 nt!KiThreadStartup+0x16

FOLLOWUP_IP:

Wdf01000!FxPkgFdo::RaiseDevicePower+50
aa4a069c 5f pop edi

SYMBOL_STACK_INDEX: 8

SYMBOL_NAME: Wdf01000!FxPkgFdo::RaiseDevicePower+50

FOLLOWUP_NAME: MachineOwner

MODULE_NAME: Wdf01000

IMAGE_NAME: Wdf01000.sys

DEBUG_FLR_IMAGE_TIMESTAMP: 4549b23a

STACK_COMMAND: .cxr 0xfffffffff89486ac ; kb

FAILURE_BUCKET_ID: 0x7E_Wdf01000!FxPkgFdo::RaiseDevicePower+50

BUCKET_ID: 0x7E_Wdf01000!FxPkgFdo::RaiseDevicePower+50

Followup: MachineOwner

Re: Standby-Sleep Problem