

# Re: Unhandled exception when pushing esi

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-05/msg00799.1>

---

- *From:* "Ivan Brugiolo [MSFT]" <[Ivan.Brugiolo@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:Ivan.Brugiolo@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 27 May 2006 12:57:40 -0700
- 

My wild guess would be that you have exhausted the kernel stack for that thread, by either creating a large on-the-stack variable, of, by calling some \_alloca() derivative function.

--  
--

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>

<[wong.kam.keung@xxxxxxxxxx](mailto:wong.kam.keung@xxxxxxxxxx)> wrote in message  
[news:1148751857.764158.51610@xx](mailto:news:1148751857.764158.51610@xx)

Hi all,

Any help will be appreciated. I got an unhandled exception in my mini file filter driver but I don't know what is causing that. The exception location reported is at a push statement and I don't understand how that will cause an exception.

```
kd> !analyze -v
```

```

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

```

KMODE\_EXCEPTION\_NOT\_HANDLED (1e)

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:

Re: Unhandled exception when pushing esi

Arg1: c0000005, The exception code that was not handled  
Arg2: f03a5ee7, The address that the exception occurred at  
Arg3: 00000001, Parameter 0 of the exception  
Arg4: 313d92f1, Parameter 1 of the exception

Debugging Details:

-----  
The call to LoadLibrary(kdextx86) failed, Win32 error 2  
"The system cannot find the file specified."  
Please check your debugger configuration and/or network access.  
The call to LoadLibrary(kdextx86) failed, Win32 error 2  
"The system cannot find the file specified."  
Please check your debugger configuration and/or network access.  
The call to LoadLibrary(kdextx86) failed, Win32 error 2  
"The system cannot find the file specified."  
Please check your debugger configuration and/or network access.

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

FAULTING\_IP:  
MyFilterDrv!CStr::Cat+9 [F:\MyFilterDrv\str.h @ 751]  
f03a5ee7 56 push esi

EXCEPTION\_PARAMETER1: 00000001

EXCEPTION\_PARAMETER2: 313d92f1

WRITE\_ADDRESS: The call to LoadLibrary(kdextx86) failed, Win32 error 2  
"The system cannot find the file specified."  
Please check your debugger configuration and/or network access.  
313d92f1

DEFAULT\_BUCKET\_ID: INTEL\_CPU\_MICROCODE\_ZERO

BUGCHECK\_STR: 0x1E

EXCEPTION\_RECORD: f0b825d4 -- (.exr ffffffff0b825d4)  
ExceptionAddress: f03a5ee7 (MyFilterDrv!CStr::Cat+0x00000009)  
ExceptionCode: c0000005 (Access violation)  
ExceptionFlags: 00000000  
NumberParameters: 2  
Parameter[0]: 00000001  
Parameter[1]: 313d92f1  
Attempt to write to address 313d92f1

LAST\_CONTROL\_TRANSFER: from 80465b11 to 8042eee4

STACK\_TEXT:  
f0b825b8 80465b11 f0b825d4 00000000 f0b82628

Re: Unhandled exception when pushing esi

nt!KiDispatchException+0x30e  
f0b82620 80465ac2 00000000 00000000 00000001  
nt!CommonDispatchException+0x4d  
f0b8264c f03ada4f f0b826cc 00000000 00000023  
nt!KiUnexpectedInterruptTail+0x207  
f0b8269c f03a6e62 f0b826cc ffffffff e2184f54  
MyFilterDrv!RtlStringCbCopyNW+0x29  
[d:\srvrtm\public\ddk\inc\ntstrsafe.h @ 1330]  
f0b826b0 f03ac0c4 f0b826cc 00000001 8117ed44  
MyFilterDrv!CStr::operator+=+0x18 [F:\MyFilterDrv\str.h @ 217]  
f0b828f0 f03ac728 e2184f54 81338790 81391d00 MyFilterDrv!GetPath+0x84  
[F:\MyFilterDrv\MyMiniDrv.cpp @ 1356]  
f0b82b64 f9d4c941 8117ed44 f0b82b84 f0b82ba0  
MyFilterDrv!My\_PreOperationCallback+0x1c4 [F:\MyFilterDrv\MyMiniDrv.cpp  
@ 655]  
f0b82bc8 f9d50162 f0b82c00 8116a4c8 00000000  
fltmgr!FltpPerformPreCallbacks+0x24c  
f0b82bdc f9d5012b f0b82c10 00000000 8127cdc0  
fltmgr!FltpPassThroughInternal+0x30  
f0b82bf8 f9d507d1 f0b82c00 8127cdc0 8118c008  
fltmgr!FltpPassThrough+0x1f1  
f0b82c28 8041ddeb 8127cdc0 8118c008 8118c008 fltmgr!FltpDispatch+0xfd  
f0b82c3c 804aea0c 8118c198 00000000 8118c008 nt!IopfCallDriver+0x35  
f0b82c50 804abb25 8127cdc0 8118c008 8116a4c8  
nt!IopSynchronousServiceTail+0x60  
f0b82d38 80465014 000002f0 00000000 00000000 nt!NtWriteFile+0x657  
f0b82d38 77f88f43 000002f0 00000000 00000000 nt!KiSystemService+0xc4  
00acf5a0 7c5864ad 000002f0 00000000 00000000 ntdll!NtWriteFile+0xb  
00acf60c 010410df 000002f0 00acf648 00000071 KERNEL32!WriteFile+0x111  
00acf638 0104145a 00000000 00acf648 7372463c ntfrs!DebPrintLine+0xfe  
00acf848 01070018 00000000 0101f9e0 0101fa1c ntfrs!DebPrint+0x53  
00acf880 010558c8 01618110 00acf89c 010ba1e0  
ntfrs!FrsHashCalcString+0x78  
00acf8a4 01068820 01620f80 01618110 00acf93c ntfrs!QHashLookupLock+0x1b  
00acf938 77d5d899 00081650 01600420 02020202  
ntfrs!SERVER\_FrsRpcSendCommPkt+0x1a6  
00acf954 77d9c912 0106867a 00acfaf8 00000002 RPCRT4!Invoke+0x30  
00acfd48 77d9c6d1 00000000 00000000 000816b4 RPCRT4!NdrStubCall2+0x664  
00acfd64 77d5d5da 000816b4 000834e8 000816b4 RPCRT4!NdrServerCall2+0x17  
00acfd9c 77d5d543 010a63b8 000816b4 00acfe40  
RPCRT4!DispatchToStubInC+0x84  
00acfd48 77d5d44e 00000000 00000000 00acfe40  
RPCRT4!RPC\_INTERFACE::DispatchToStubWorker+0x100  
00acfe14 77d53f52 000816b4 00000000 00acfe40  
RPCRT4!RPC\_INTERFACE::DispatchToStub+0x5e  
00acfe44 77d53e93 00000000 000817b0 00081650  
RPCRT4!OSF\_SCALL::DispatchHelper+0xaf  
00acfe58 77d53e16 00000000 00000000 7c57b580  
RPCRT4!OSF\_SCALL::DispatchRPCCall+0x121  
00acfe90 77d53d13 000bff80 00000303 00000000  
RPCRT4!OSF\_SCALL::ProcessReceivedPDU+0x46

Re: Unhandled exception when pushing esi

00acfeb0 77d53460 000bff80 0000032d 00015f90  
RPCRT4!OSF\_SCALL::BeginRpcCall+0x1f5  
00acff10 77d533a8 00000000 000bff80 0000032d  
RPCRT4!OSF\_SCONNECTION::ProcessReceiveComplete+0x52d  
00acff20 77d4f99c 00078d08 0000000c 00000000  
RPCRT4!ProcessConnectionServerReceivedEvent+0x1b  
00acff74 77d43dd7 77d4e003 00078d08 000985e0  
RPCRT4!LOADABLE\_TRANSPORT::ProcessIOEvents+0x14a  
00acff78 77d4e003 00078d08 000985e0 53570000  
RPCRT4!ProcessIOEventsWrapper+0x9  
00acffa8 77d4af16 00082f70 00acffec 7c57b388  
RPCRT4!BaseCachedThreadRoutine+0x4f  
00acffb4 7c57b388 0007b338 000985e0 53570000  
RPCRT4!ThreadStartRoutine+0x18  
00acffec 00000000 77d4aefc 0007b338 00000000  
KERNEL32!BaseThreadStart+0x52

STACK\_COMMAND: .bugcheck ; kb

FOLLOWUP\_IP:

MyFilterDrv!CStr::Cat+9 [F:\MyFilterDrv\str.h @ 751]  
f03a5ee7 56 push esi

FAULTING\_SOURCE\_CODE:

747: }  
748:  
749: bool Cat(LPCWSTR str, int nLength = -1)  
750: {  
  
751: if (!str)  
  
752: return true;  
753:  
754: if (nLength == -1)  
755: nLength = wcslen(str) \* sizeof(WCHAR);  
756:

FOLLOWUP\_NAME: MachineOwner

SYMBOL\_NAME: MyFilterDrv!CStr::Cat+9

MODULE\_NAME: MyFilterDrv

IMAGE\_NAME: MyFilterDrv.sys

DEBUG\_FLR\_IMAGE\_TIMESTAMP: 4464ddea

FAILURE\_BUCKET\_ID: 0x1E\_W\_MyFilterDrv!CStr::Cat+9

Re: Unhandled exception when pushing esi

BUCKET\_ID: 0x1E\_W\_MyFilterDrv!CStr::Cat+9

Followup: MachineOwner  
-----

VirtualToOffset: 113d92f1 not properly sign extended

[...]

kd> kv

ChildEBP RetAddr Args to Child

f0b825b8 80465b11 f0b825d4 00000000 f0b82628

nt!KiDispatchException+0x30e (FPO: [Non-Fpo])

f0b82620 80465ac2 00000000 00000000 00000001

nt!CommonDispatchException+0x4d (FPO: [0,20,0])

f0b8264c f03ada4f f0b826cc 00000000 00000023

nt!KiUnexpectedInterruptTail+0x207

f0b8269c f03a6e62 f0b826cc ffffffff e2184f54

MyFilterDrv!RtlStringCbCopyNW+0x29 (FPO: [Non-Fpo]) (CONV: stdcall)

[d:\srvrtm\public\ddk\inc\ntstrsafe.h @ 1330]

f0b826b0 f03ac0c4 f0b826cc 00000001 8117ed44

MyFilterDrv!CStr::operator+=+0x18 (FPO: [Non-Fpo]) (CONV: thiscall)

[F:\MyFilterDrv\str.h @ 217]

f0b828f0 f03ac728 e2184f54 81338790 81391d00 MyFilterDrv!GetPath+0x84

(FPO: [Non-Fpo]) (CONV: stdcall) [F:\MyFilterDrv\MyMiniDrv.cpp @ 1356]

f0b82b64 f9d4c941 8117ed44 f0b82b84 f0b82ba0

MyFilterDrv!My\_PreOperationCallback+0x1c4 (FPO: [Non-Fpo]) (CONV:

stdcall) [F:\MyFilterDrv\MyMiniDrv.cpp @ 655]

f0b82bc8 f9d50162 f0b82c00 8116a4c8 00000000

fltmgr!FltpPerformPreCallbacks+0x24c (FPO: [Non-Fpo])

f0b82bdc f9d5012b f0b82c10 00000000 8127cdc0

fltmgr!FltpPassThroughInternal+0x30 (FPO: [2,0,3])

f0b82bf8 f9d507d1 f0b82c00 8127cdc0 8118c008

fltmgr!FltpPassThrough+0x1f1 (FPO: [Non-Fpo])

f0b82c28 8041ddeb 8127cdc0 8118c008 8118c008 fltmgr!FltpDispatch+0xfd

(FPO: [Non-Fpo])

f0b82c3c 804aea0c 8118c198 00000000 8118c008 nt!IopfCallDriver+0x35

(FPO: [0,0,2])

f0b82c50 804abb25 8127cdc0 8118c008 8116a4c8

nt!IopSynchronousServiceTail+0x60 (FPO: [Non-Fpo])

f0b82d38 80465014 000002f0 00000000 00000000 nt!NtWriteFile+0x657 (FPO:

[Non-Fpo])

f0b82d38 77f88f43 000002f0 00000000 00000000 nt!KiSystemService+0xc4

(FPO: [0,0] TrapFrame @ f0b82d64)

00acf5a0 7c5864ad 000002f0 00000000 00000000 ntdll!NtWriteFile+0xb

(FPO: [9,0,0])

00acf60c 010410df 000002f0 00acf648 00000071 KERNEL32!WriteFile+0x111

(FPO: [Non-Fpo])

00acf638 0104145a 00000000 00acf648 7372463c ntfrs!DebPrintLine+0xfe

(FPO: [Uses EBP] [2,1,4])

00acf848 01070018 00000000 0101f9e0 0101fa1c ntfrs!DebPrint+0x53 (FPO:

Re: Unhandled exception when pushing esi

```
[Non-Fpo]
00acf880 010558c8 01618110 00acf89c 010ba1e0
ntfrs!FrsHashCalcString+0x78 (FPO: [Non-Fpo])
kd> .trap f0b82628
ErrCode = 00000002
eax=f0b826cc ebx=81391d00 ecx=81391d00 edx=f0b82702 esi=81391d00
edi=e2184f5c
eip=f03a5ee7 esp=f0b8269c ebp=f0b8269c iopl=0 nv up ei ng nz na
po nc
cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000
efl=00010286
MyFilterDrv!CStr::Cat+0x9:
0008:f03a5ee7 56 push esi
kd> kv
*** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr Args to Child
f0b8269c f03a6e62 f0b826cc ffffffff e2184f54 MyFilterDrv!CStr::Cat+0x9
(FPO: [Non-Fpo]) (CONV: thiscall) [F:\MyFilterDrv\str.h @ 751]
f0b826b0 f03ac0c4 f0b826cc 00000001 8117ed44
MyFilterDrv!CStr::operator+=+0x18 (FPO: [Non-Fpo]) (CONV: thiscall)
[F:\MyFilterDrv\str.h @ 217]
f0b828f0 f03ac728 e2184f54 81338790 81391d00 MyFilterDrv!GetPath+0x84
(FPO: [Non-Fpo]) (CONV: stdcall) [F:\MyFilterDrv\MyMiniDrv.cpp @ 1356]
f0b82b64 f9d4c941 8117ed44 f0b82b84 f0b82ba0
MyFilterDrv!My_PreOperationCallback+0x1c4 (FPO: [Non-Fpo]) (CONV:
stdcall) [F:\MyFilterDrv\MyMiniDrv.cpp @ 655]
f0b82bc8 f9d50162 f0b82c00 8116a4c8 00000000
fltmgr!FltpPerformPreCallbacks+0x24c (FPO: [Non-Fpo])
f0b82bdc f9d5012b f0b82c10 00000000 8127cdc0
fltmgr!FltpPassThroughInternal+0x30 (FPO: [2,0,3])
f0b82bf8 f9d507d1 f0b82c00 8127cdc0 8118c008
fltmgr!FltpPassThrough+0x1f1 (FPO: [Non-Fpo])
f0b82c28 8041ddeb 8127cdc0 8118c008 8118c008 fltmgr!FltpDispatch+0xfd
(FPO: [Non-Fpo])
f0b82c3c 804aea0c 8118c198 00000000 8118c008 nt!IopfCallDriver+0x35
(FPO: [0,0,2])
f0b82c50 804abb25 8127cdc0 8118c008 8116a4c8
nt!IopSynchronousServiceTail+0x60 (FPO: [Non-Fpo])
f0b82d38 80465014 000002f0 00000000 00000000 nt!NtWriteFile+0x657 (FPO:
[Non-Fpo])
f0b82d38 77f88f43 000002f0 00000000 00000000 nt!KiSystemService+0xc4
(FPO: [0,0] TrapFrame @ f0b82d64)
00acf5a0 7c5864ad 000002f0 00000000 00000000 ntdll!NtWriteFile+0xb
(FPO: [9,0,0])
00acf60c 010410df 000002f0 00acf648 00000071 KERNEL32!WriteFile+0x111
(FPO: [Non-Fpo])
00acf638 0104145a 00000000 00acf648 7372463c ntfrs!DebPrintLine+0xfe
(FPO: [Uses EBP] [2,1,4])
00acf848 01070018 00000000 0101f9e0 0101fa1c ntfrs!DebPrint+0x53 (FPO:
[Non-Fpo])
00acf880 010558c8 01618110 00acf89c 010ba1e0
```

Re: Unhandled exception when pushing esi

```
ntfrs!FrsHashCalcString+0x78 (FPO: [Non-Fpo])  
00acf8a4 01068820 01620f80 01618110 00acf93c ntfrs!QHashLookupLock+0x1b  
(FPO: [Non-Fpo])  
00acf938 77d5d899 00081650 01600420 02020202  
ntfrs!SERVER_FrsRpcSendCommPkt+0x1a6 (FPO: [Non-Fpo])  
00acf954 77d9c912 0106867a 00acfaf8 00000002 RPCRT4!Invoke+0x30
```

```
MyFilterDrv!CStr::Cat:  
f03a5ede 8bff mov edi,edi  
f03a5ee0 55 push ebp  
f03a5ee1 8bec mov ebp,esp  
f03a5ee3 837d0800 cmp dword ptr [ebp+0x8],0x0  
f03a5ee7 56 push esi  
f03a5ee8 8bf1 mov esi,ecx
```