

## Re: Bugcheck D1 in NDIS-WDM driver

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2004-12/0895.html>

---

**From:** Harshal (*harshal\_at\_gmail.com*)

**Date:** 12/20/04

Date: 20 Dec 2004 15:15:40 -0800

> *Even if you could guarantee that this code itself is serialized*  
> *(i.e. you will never have two thread running*  
`osIndicateReceiveDeserized`  
> *at the same time,) and your Queue functions are protected, you still*  
> *need to avoid the gaps between check, get and remove above because*  
> *your ReturnPacket handler can kick in-between and changes your*  
> *queue. In particular description of your bug (the bugcheck happens*  
> *when you have a lot of packet to indicate) points to lack of list*  
> *protection and serialization issues in your code.*

Ali,

Thanks for pointing out the lack of locks around the queue accesses. I have now added spinlocks in this routine and also in the return packet handler. This seems to have fixed this particular problem. BTW, when I mentioned 200 packets, I meant that the driver has successfully processed more than 200 packets. I did not mean to imply that 200 packets are waiting to be indicated to NDIS. Sorry for the confusion.

When I use the verifier to further test this driver, I see various other bugchecks in some other OS modules. I am guessing that these are all related to my driver (I doubt that `ntfs.sys` or `ntoskrnl.exe` have bugs) but I can't pinpoint the problem. I have two PCs that load this driver and use it to 'ping' each other. One of the PCs stopped with a `NTFS_FILE_SYSTEM (24)` bugcheck and the other with a `IRQL_NOT_LESS_OR_EQUAL (a)`. None of the stack traces has an entry for my driver. I have included the details below. How do I back trace the problem to a routine in my driver that caused the problem?

Thanks,  
- Harshal

1. PC #1

BugCheck A, {4, 2, 1, 804eca25}

\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols  
for fsinvprv.dll -  
Probably caused by : ntoskrnl.exe ( nt!KiInsertTimerTable+52 )

Followup: MachineOwner  
-----

nt!RtlpBreakWithStatusInstruction:

80510b26 cc int 3

kd> !analyze -v

\*\*\*\*\*

\*

\*

\* Bugcheck Analysis

\*

\*

\*

\*\*\*\*\*

IRQL\_NOT\_LESS\_OR\_EQUAL (a)

An attempt was made to access a pageable (or completely invalid)  
address at an

interrupt request level (IRQL) that is too high. This is usually  
caused by drivers using improper addresses.

If a kernel debugger is available get the stack backtrace.

Arguments:

Arg1: 00000004, memory referenced

Arg2: 00000002, IRQL

Arg3: 00000001, value 0 = read operation, 1 = write operation

Arg4: 804eca25, address which referenced memory

Debugging Details:  
-----

OVERLAPPED\_MODULE: rdbss

WRITE\_ADDRESS: 00000004

CURRENT\_IRQL: 2

FAULTING\_IP:

nt!KiInsertTimerTable+52

804eca25 894a04 mov [edx+0x4],ecx

DEFAULT\_BUCKET\_ID: DRIVER\_FAULT

BUGCHECK\_STR: 0xA

LAST\_CONTROL\_TRANSFER: from 804ec9cf to 804eca25

TRAP\_FRAME: b23fdc40 --- (.trap ffffffff23fdc40)  
ErrCode = 00000002  
eax=80540100 ebx=832b63e8 ecx=832b6490 edx=00000000 esi=8054cc08  
edi=832b6440  
eip=804eca25 esp=b23fdcb4 ebp=b23fdcbc iopl=0 nv up ei ng nz ac  
pe cy  
cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000  
efl=00010293  
nt!KiInsertTimerTable+0x52:  
804eca25 894a04 mov [edx+0x4],ecx  
Resetting default scope

STACK\_TEXT:

b23fdcbc 804ec9cf ffff1e0 ffffffff f97704b0 nt!KiInsertTimerTable+0x52  
b23fdcd8 804ec1d6 ffff1e0 ffffffff b23fdd64 nt!KiInsertTreeTimer+0x8a  
b23fdd0c 80582026 b23fdc01 00000000 b23fdd30  
nt!KeDelayExecutionThread+0xec  
b23fdd54 804da1dd 00000000 007ae560 00000000 nt!NtDelayExecution+0x87  
b23fdd54 7ffe0304 00000000 007ae560 00000000 nt!KiSystemService+0xc4  
007ae538 77f5b7f4 77e7a2cd 00000000 007ae560  
SharedUserData!SystemCallStub+0x4  
007ae53c 77e7a2cd 00000000 007ae560 18351d88 ntdll!ZwDelayExecution+0xc  
007ae594 77e61bf5 00000002 00000000 183575c8 kernel32!SleepEx+0x61  
007ae5a0 183575c8 00000002 000003e3 77c43df0 kernel32!Sleep+0xb  
WARNING: Stack unwind information not available. Following frames may  
be wrong.  
007ae8b0 1835784f 00af07aa 18351d88 00000000  
fsinvprv!DllGetClassObject+0x33db  
007aeb58 18357870 00af13f2 000b6330 18351d88  
fsinvprv!DllGetClassObject+0x3662  
007aee04 18357870 00af0ff2 000b6638 00000000  
fsinvprv!DllGetClassObject+0x3683  
007af0b0 18357b1f 00af1390 000b6f30 18351d88  
fsinvprv!DllGetClassObject+0x3683  
007af0e0 18357ed4 00af0c02 00000001 00af06b8  
fsinvprv!DllGetClassObject+0x3932  
007af350 183566de 00af0da0 773d0000 000ad840  
fsinvprv!DllGetClassObject+0x3ce7  
007af4e0 010184c0 00aef000 000aa7e4 000b59a4  
fsinvprv!DllGetClassObject+0x24f1  
007af560 01018664 00000000 000aa7fc 000b54cc  
wmiprvse!CInterceptor\_IWbemSyncProvider::Helper\_ExecQueryAsync+0x48a  
007af5a8 780038f7 00aef000 000aa7fc 000b54cc  
wmiprvse!CInterceptor\_IWbemSyncProvider::ExecQueryAsync+0x83  
007af5d4 780791a5 010185e1 007af5e8 00000006 RPCRT4!Invoke+0x30  
007af9c8 78079e0c 000b3b70 000abe70 00099d74 RPCRT4!NdrStubCall2+0x1fb  
007afa20 756bc294 000b3b70 00099d74 000abe70  
RPCRT4!CStdStubBuffer\_Invoke+0xc6  
007afa30 772b8c2e 00501164 00099d74 000abe70  
FastProx!CBaseStublet::Invoke+0x1c  
007afa70 772b8bdd 00099d74 000b3a78 00096128 OLE32!SyncStubInvoke+0x33

microsoft.public.development.device.drivers: Re: Bugcheck D1 in NDIS-WDM driver

007afab8 771dfa39 00099d74 000aa9b8 00501164 OLE32!StubInvoke+0xa5  
007afb90 771df963 000abe70 00000000 00501164  
OLE32!CCtxComChnl::ContextInvoke+0xe3  
007afbac 772b8b1a 00099d74 00000001 00501164 OLE32!MTAInvoke+0x18  
007afdbc 772b89d4 00099d20 000abe70 00501164 OLE32!AppInvoke+0x9a  
007afca4 772b8eb3 00098958 000b5050 00000000  
OLE32!ComInvokeWithLockAndIPID+0x2b3  
007afce8 78002d28 00099d20 00000000 000006bb OLE32!ThreadInvoke+0x1c3  
007afd1c 78002ca5 772b8d78 00099c94 007afdfc  
RPCRT4!DispatchToStubInC+0x38  
007afd78 78002baf 00099c94 00000000 771bf63c  
RPCRT4!RPC\_INTERFACE::DispatchToStubWorker+0x132  
007afd9c 780123e5 00099c94 00000000 771bf63c  
RPCRT4!RPC\_INTERFACE::DispatchToStub+0x82  
007afdcc 78012424 00099c94 00099c50 00000000  
RPCRT4!RPC\_INTERFACE::DispatchToStubWithObject+0xb3  
007afe08 780091be 00099a40 80030001 000940d0  
RPCRT4!LRPC\_SCALL::DealWithRequestMessage+0x342  
007afe2c 78001721 00091624 007afe48 00099a40  
RPCRT4!LRPC\_ADDRESS::DealWithLRPCRequest+0x16b  
007aff90 78001601 780019d4 000915e8 77fa88f0  
RPCRT4!LRPC\_ADDRESS::ReceiveLotsaCalls+0x298  
007aff94 780019d4 000915e8 77fa88f0 00091708  
RPCRT4!RecvLotsaCallsWrapper+0x9  
007affac 780015f3 000917e0 77e7d28e 00091808  
RPCRT4!BaseCachedThreadRoutine+0x64  
007affb4 77e7d28e 00091808 77fa88f0 00091708  
RPCRT4!ThreadStartRoutine+0x16  
007affec 00000000 780015dd 00091808 00000000  
kernel32!BaseThreadStart+0x37

FOLLOWUP\_IP:

nt!KiInsertTimerTable+52  
804eca25 894a04 mov [edx+0x4],ecx

SYMBOL\_STACK\_INDEX: 0

FOLLOWUP\_NAME: MachineOwner

SYMBOL\_NAME: nt!KiInsertTimerTable+52

MODULE\_NAME: nt

IMAGE\_NAME: ntoskrnl.exe

DEBUG\_FLR\_IMAGE\_TIMESTAMP: 40d1d336

STACK\_COMMAND: .trap ffffffff23fdc40 ; kb

FAILURE\_BUCKET\_ID: 0xA\_W\_VRF\_nt!KiInsertTimerTable+52

microsoft.public.development.device.drivers: Re: Bugcheck D1 in NDIS-WDM driver

BUCKET\_ID: 0xA\_W\_VRF\_nt!KiInsertTimerTable+52

Followup: MachineOwner  
-----

2. PC #2

BugCheck 24, {1902fa, f9c43910, f9c43610, baed6d12}

Loading symbols for baeb2000 Ntfs.sys -> Ntfs.sys  
Probably caused by : Ntfs.sys ( Ntfs!NtfsCheckpointVolume+63e )

Followup: MachineOwner  
-----

nt!RtlpBreakWithStatusInstruction:

80510b26 cc int 3

kd> !analyze -v

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

NTFS\_FILE\_SYSTEM (24)

If you see NtfsExceptionFilter on the stack then the 2nd and 3rd parameters are the exception record and context record. Do a .cxr on the 3rd parameter and then kb to obtain a more informative stack trace.

Arguments:

Arg1: 001902fa

Arg2: f9c43910

Arg3: f9c43610

Arg4: baed6d12

Debugging Details:  
-----

EXCEPTION\_RECORD: f9c43910 --- (.cxr ffffffff9c43910)  
ExceptionAddress: baed6d12 (Ntfs!NtfsCheckpointVolume+0x0000063e)  
ExceptionCode: c0000005 (Access violation)  
ExceptionFlags: 00000000  
NumberParameters: 2  
Parameter[0]: 00000000  
Parameter[1]: 00000078  
Attempt to read from address 00000078

microsoft.public.development.device.drivers: Re: Bugcheck D1 in NDIS-WDM driver

CONTEXT: f9c43610 --- (.cxr ffffffff9c43610)  
eax=81342158 ebx=81956850 ecx=00000064 edx=00000028 esi=00000000  
edi=804ecee6  
eip=baed6d12 esp=f9c439d8 ebp=f9c43be0 iopl=0 nv up ei pl zr na  
po nc  
cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000  
efl=00010246  
Ntfs!NtfsCheckpointVolume+0x63e:  
baed6d12 668b4914 mov cx,[ecx+0x14]  
Resetting default scope

DEFAULT\_BUCKET\_ID: DRIVER\_FAULT

BUGCHECK\_STR: 0x24

LAST\_CONTROL\_TRANSFER: from baed7334 to baed6d12

STACK\_TEXT:

f9c43be0 baed7334 f9c43c4c 81956850 00000000  
Ntfs!NtfsCheckpointVolume+0x63e  
f9c43d74 804ed99f 00000000 00000000 8194cda8  
Ntfs!NtfsCheckpointAllVolumes+0xff  
f9c43dac 8057dfe1 00000000 00000000 00000000 nt!ExpWorkerThread+0xfe  
f9c43ddc 80512c12 804ed8cc 00000000 00000000  
nt!PspSystemThreadStartup+0x34  
00000000 00000000 00000000 00000000 00000000 nt!KiThreadStartup+0x16

FOLLOWUP\_IP:

Ntfs!NtfsCheckpointVolume+63e  
baed6d12 668b4914 mov cx,[ecx+0x14]

SYMBOL\_STACK\_INDEX: 0

FOLLOWUP\_NAME: MachineOwner

SYMBOL\_NAME: Ntfs!NtfsCheckpointVolume+63e

MODULE\_NAME: Ntfs

IMAGE\_NAME: Ntfs.sys

DEBUG\_FLR\_IMAGE\_TIMESTAMP: 3d6de5c1

STACK\_COMMAND: .cxr ffffffff9c43610 ; kb

FAILURE\_BUCKET\_ID: 0x24\_Ntfs!NtfsCheckpointVolume+63e

BUCKET\_ID: 0x24\_Ntfs!NtfsCheckpointVolume+63e

Followup: MachineOwner

-----