

RE: NDIS filter driver crash during bootup

Source:

[http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-03/msg00352.h](http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-03/msg00352.html)

- *From:* mirage2k2 <mirage2k2@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 14 Mar 2006 20:02:26 -0800
-

Have you tried disabling any antivirus software that might be running (as the help on bugcheck 50 suggests)?

Can you get hold of a copy of softice? This will allow you to step-through your driver code at boot time.

Also, if your driver has been based on a ddk example, then try using the example to see if it also crashes.

"sirip" wrote:

I have a huge IPSEC filter driver(about 30M+) that used to load and work well. Once in a while, it used to crash as follows during bootup. I was never able to consistently re-produce it to go after that. Now, it happens everytime I install this driver and reboot the machine.

Since this is during the loading of the driver itself, I am not able to figure out how to go about chasing this problem.

This is on Win2KSP4. Any pointers would be greatly appreciated.

thanks

Connected to Windows 2000 2195 x86 compatible target, ptr64 FALSE

Loading Kernel Symbols

.....

Loading unloaded module list

Loading User Symbols

*

*

* Bugcheck Analysis

*

*

*

RE: NDIS filter driver crash during bootup

Use !analyze -v to get detailed debugging information.

BugCheck 50, {e134a000, 0, 804861b7, 1}

Probably caused by : memory_corruption (nt!MiLoadImageSection+42e)

Followup: MachineOwner

nt!RtlpBreakWithStatusInstruction:

80456488 cc int 3

kd> !analyze -v

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

PAGE_FAULT_IN_NONPAGED_AREA (50)

Invalid system memory was referenced. This cannot be protected by try-except, it must be protected by a Probe. Typically the address is just plain bad or it

is pointing at freed memory.

Arguments:

Arg1: e134a000, memory referenced.

Arg2: 00000000, value 0 = read operation, 1 = write operation.

Arg3: 804861b7, If non-zero, the instruction address which referenced the bad memory address.

Arg4: 00000001, (reserved)

Debugging Details:

READ_ADDRESS: e134a000 Paged pool

FAULTING_IP:

nt!MiLoadImageSection+42e

804861b7 8b00 mov eax,[eax]

MM_INTERNAL_CODE: 1

DEFAULT_BUCKET_ID: DRIVER_FAULT

BUGCHECK_STR: 0x50

RE: NDIS filter driver crash during bootup

LAST_CONTROL_TRANSFER: from 804a0cb1 to 804861b7

TRAP_FRAME: f401f1c8 -- (.trap ffffffff401f1c8)

ErrCode = 00000000

eax=e134a000 ebx=052b9000 ecx=00001000 edx=00000000 esi=80062f10 edi=80062ea0

eip=804861b7 esp=f401f23c ebp=f401f2f4 iopl=0 nv up ei ng nz na po cy

cs=0008 ss=0010 ds=0023 es=0023 fs=0030 gs=0000 efl=00010287

nt!MiLoadImageSection+0x42e:

804861b7 8b00 mov eax,[eax]

Resetting default scope

STACK_TEXT:

f401f2f4 804a0cb1 e1344410 f401f660 f401f678 nt!MiLoadImageSection+0x42e
f401f588 804c26dc f401f678 00000000 00000000 nt!MiLoadSystemImage+0x4e2
f401f5ac 80499e21 f401f678 00000000 00000000 nt!MmLoadSystemImage+0x1c
f401f684 804277a5 80000028 00000000 e134502c nt!IopLoadDriver+0x3a3
f401f6b4 804ad78b 81863488 80000028 00000003
nt!IopCallDriverAddDeviceQueryRoutine+0x356
f401f704 804ad983 f401f790 00000010 f401f760
nt!RtlpCallQueryRegistryRoutine+0x34a
f401f768 8049afaf 00000000 00000082 00000001 nt!RtlQueryRegistryValues+0x1ed
f401f82c 80553b81 8000002c 00000001 f401f864 nt!IopCallDriverAddDevice+0x38f
f401f848 80553ada 81882808 f401f864 00000003
nt!IopProcessAddDevicesWorker+0x6c
f401f86c 805529a5 818a5b48 0000ffff 00000003 nt!IopProcessAddDevices+0x59
f401f8c0 80550f89 00000000 00000032 00000000
nt!IopInitializeSystemDrivers+0x25
f401fa58 8054fd14 80087000 00000000 00000000 nt!IoInitSystem+0x644
f401fda8 80455a16 80087000 00000000 00000000 nt!Phase1Initialization+0x71b
f401fddc 80469bb2 8054f660 80087000 00000000 nt!PspSystemThreadStartup+0x69
00000000 00000000 00000000 00000000 00000000 nt!KiThreadStartup+0x16

FOLLOWUP_IP:

nt!MiLoadImageSection+42e

804861b7 8b00 mov eax,[eax]

SYMBOL_STACK_INDEX: 0

FOLLOWUP_NAME: MachineOwner

SYMBOL_NAME: nt!MiLoadImageSection+42e

MODULE_NAME: nt

DEBUG_FLR_IMAGE_TIMESTAMP: 3ee6c002

STACK_COMMAND: .trap ffffffff401f1c8 ; kb

IMAGE_NAME: memory_corruption

RE: NDIS filter driver crash during bootup

FAILURE_BUCKET_ID: 0x50_nt!MiLoadImageSection+42e

BUCKET_ID: 0x50_nt!MiLoadImageSection+42e

Followup: MachineOwner
