

2.6.0-test4-mm2: fdisk causes Oops

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2003-08/7749.html>

From: Peter Lieverdink (cafuego_at_cc.com.au)

Date: 08/29/03

To: linux-kernel@vger.kernel.org

Date: Fri, 29 Aug 2003 15:12:52 +1000

Hi,

When running `fdisk -l` under 2.6.0-test4-mm2, the kernel oopses. `dmesg`, the oops (`fdisk.txt`) and output from `lspci` are attached.

I've tried after disabling the Promise controller in the BIOS, but the oops still occurs. Same when I specify a device instead of `-l`.

`fdisk` is from `debian/unstable`, version 2.11z

– Peter.

Linux version 2.6.0-test4-mm2 (root@kahlua) (gcc version 3.3.2 20030812 (Debian prerelease)) #1 Fri Aug 29 10:07:13 EST 2003

Video mode to be used for restore is f00

BIOS-provided physical RAM map:

BIOS-e820: 0000000000000000 – 000000000009fc00 (usable)
BIOS-e820: 000000000009fc00 – 00000000000a0000 (reserved)
BIOS-e820: 00000000000f0000 – 0000000000100000 (reserved)
BIOS-e820: 0000000000100000 – 000000003fff0000 (usable)
BIOS-e820: 000000003fff0000 – 000000003fff3000 (ACPI NVS)
BIOS-e820: 000000003fff3000 – 0000000040000000 (ACPI data)
BIOS-e820: 00000000fec00000 – 00000000fec01000 (reserved)
BIOS-e820: 00000000fee00000 – 00000000fee01000 (reserved)
BIOS-e820: 00000000ffff0000 – 0000000100000000 (reserved)

127MB HIGHMEM available.

896MB LOWMEM available.

found SMP MP-table at 000f4db0

hm, page 000f4000 reserved twice.

hm, page 000f5000 reserved twice.

hm, page 000f0000 reserved twice.

hm, page 000f1000 reserved twice.

On node 0 totalpages: 262128

DMA zone: 4096 pages, LIFO batch:1

Normal zone: 225280 pages, LIFO batch:16

Linux–Kernel: 2.6.0–test4–mm2: fdisk causes Oops

HighMem zone: 32752 pages, LIFO batch:7
DMI 2.3 present.
ACPI: RSDP (v000 GBT) @ 0x000f6730
ACPI: RSDT (v001 GBT AWRDACPI 0x42302e31 AWRD 0x01010101) @ 0x3fff3000
ACPI: FADT (v001 GBT AWRDACPI 0x42302e31 AWRD 0x01010101) @ 0x3fff3040
ACPI: MADT (v001 GBT AWRDACPI 0x42302e31 AWRD 0x01010101) @ 0x3fff7280
ACPI: DSDT (v001 GBT AWRDACPI 0x00001000 MSFT 0x0100000c) @ 0x00000000
ACPI: Local APIC address 0xfe00000
ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Processor #0 6:8 APIC version 16
ACPI: LAPIC_NMI (acpi_id[0x00] polarity[0x0] trigger[0x0] lint[0x1])
Using ACPI for processor (LAPIC) configuration information
Intel MultiProcessor Specification v1.4
Virtual Wire compatibility mode.
OEM ID: OEM00000 Product ID: PROD00000000 APIC at: 0xFEE00000
I/O APIC #2 Version 17 at 0xFEC00000.
Enabling APIC mode: Flat. Using 1 I/O APICs
Processors: 1
Building zonelist for node : 0
Kernel command line: root=/dev/hda2 pci=noacpi
current: c036c9c0
current->thread_info: c03c6000
Initializing CPU#0
PID hash table entries: 4096 (order 12: 32768 bytes)
Detected 2009.462 MHz processor.
Console: colour VGA+ 80x25
Calibrating delay loop... 3956.73 BogomIPS
Memory: 1033740k/1048512k available (2045k kernel code, 13832k reserved, 791k data, 368k init, 131008k highmem)
zapping low mappings.
Dentry cache hash table entries: 131072 (order: 7, 524288 bytes)
Inode-cache hash table entries: 65536 (order: 6, 262144 bytes)
Mount-cache hash table entries: 512 (order: 0, 4096 bytes)
-> /dev
-> /dev/console
-> /root
CPU: After generic identify, caps: 0383fbff c1c3fbff 00000000 00000000
CPU: After vendor identify, caps: 0383fbff c1c3fbff 00000000 00000000
CPU: L1 I Cache: 64K (64 bytes/line), D cache 64K (64 bytes/line)
CPU: L2 Cache: 256K (64 bytes/line)
CPU: After all inits, caps: 0383fbff c1c3fbff 00000000 00000020
Intel machine check architecture supported.
Intel machine check reporting enabled on CPU#0.
CPU: AMD Athlon(tm) XP 2400+ stepping 01
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
enabled ExtINT on CPU#0
ESR value before enabling vector: 00000000
ESR value after enabling vector: 00000000

```
ENABLING IO-APIC IRQs
Setting 2 in the phys_id_present_map
...changing IO-APIC physical APIC ID to 2 ... ok.
init IO-APIC IRQs
IO-APIC (apicid=pin) 2-0, 2-6, 2-7, 2-10, 2-11, 2-17, 2-20, 2-23 not connected.
..TIMER: vector=0x31 pin1=2 pin2=0
number of MP IRQ sources: 23.
number of IO-APIC #2 registers: 24.
testing the IO APIC.....
IO APIC #2.....
.... register #00: 02000000
..... : physical APIC id: 02
..... : Delivery Type: 0
..... : LTS : 0
.... register #01: 00178003
..... : max redirection entries: 0017
..... : PRQ implemented: 1
..... : IO APIC version: 0003
.... IRQ redirection table:
NR Log Phy Mask Trig IRR Pol Stat Dest Deli Vect:
00 000 00 1 0 0 0 0 0 0 00
01 001 01 0 0 0 0 0 1 1 39
02 001 01 0 0 0 0 0 1 1 31
03 001 01 0 0 0 0 0 1 1 41
04 001 01 0 0 0 0 0 1 1 49
05 001 01 0 0 0 0 0 1 1 51
06 000 00 1 0 0 0 0 0 0 00
07 000 00 1 0 0 0 0 0 0 00
08 001 01 0 0 0 0 0 1 1 59
09 001 01 0 0 0 0 0 1 1 61
0a 000 00 1 0 0 0 0 0 0 00
0b 000 00 1 0 0 0 0 0 0 00
0c 001 01 0 0 0 0 0 1 1 69
0d 001 01 0 0 0 0 0 1 1 71
0e 001 01 0 0 0 0 0 1 1 79
0f 001 01 0 0 0 0 0 1 1 81
10 001 01 1 1 0 1 0 1 1 89
11 000 00 1 0 0 0 0 0 0 00
12 001 01 1 1 0 1 0 1 1 91
13 001 01 1 1 0 1 0 1 1 99
14 000 00 1 0 0 0 0 0 0 00
15 001 01 1 1 0 1 0 1 1 A1
16 001 01 1 1 0 1 0 1 1 A9
17 000 00 1 0 0 0 0 0 0 00
IRQ to pin mappings:
IRQ0 -> 0:2
IRQ1 -> 0:1
IRQ3 -> 0:3
IRQ4 -> 0:4
IRQ5 -> 0:5
IRQ8 -> 0:8
```

```
IRQ9 -> 0:9
IRQ12 -> 0:12
IRQ13 -> 0:13
IRQ14 -> 0:14
IRQ15 -> 0:15
IRQ16 -> 0:16
IRQ18 -> 0:18
IRQ19 -> 0:19
IRQ21 -> 0:21
IRQ22 -> 0:22
..... done.
Using local APIC timer interrupts.
calibrating APIC timer ...
..... CPU clock speed is 2008.0925 MHz.
..... host bus clock speed is 267.0856 MHz.
PM: Adding info for No Bus:legacy
Initializing RT netlink socket
PCI: PCI BIOS revision 2.10 entry at 0xfa050, last bus=1
PCI: Using configuration type 1
mtrr: v2.0 (20020519)
ACPI: Subsystem revision 20030813
ACPI: Interpreter enabled
ACPI: Using PIC for interrupt routing
ACPI: PCI Root Bridge [PCI0] (00:00)
PCI: Probing PCI hardware (bus 00)
PM: Adding info for No Bus:pci0000:00
PM: Adding info for pci:0000:00:00.0
PM: Adding info for pci:0000:00:01.0
PM: Adding info for pci:0000:00:0a.0
PM: Adding info for pci:0000:00:0b.0
PM: Adding info for pci:0000:00:0b.1
PM: Adding info for pci:0000:00:0f.0
PM: Adding info for pci:0000:00:10.0
PM: Adding info for pci:0000:00:10.1
PM: Adding info for pci:0000:00:10.2
PM: Adding info for pci:0000:00:10.3
PM: Adding info for pci:0000:00:11.0
PM: Adding info for pci:0000:00:11.1
PM: Adding info for pci:0000:00:11.5
PM: Adding info for pci:0000:00:13.0
PM: Adding info for pci:0000:00:14.0
PM: Adding info for pci:0000:01:00.0
ACPI: PCI Interrupt Routing Table [_SB_.PCI0._PRT]
ACPI: PCI Interrupt Link [LNKA] (IRQs 1 3 4 5 6 *7 10 11 12 14 15)
ACPI: PCI Interrupt Link [LNKB] (IRQs 1 3 4 5 *6 7 10 11 12 14 15)
ACPI: PCI Interrupt Link [LNKC] (IRQs 1 3 4 5 6 7 *10 11 12 14 15)
ACPI: PCI Interrupt Link [LNKD] (IRQs 1 3 4 5 6 7 10 *11 12 14 15)
ACPI: PCI Interrupt Link [ALKA] (IRQs 20, disabled)
ACPI: PCI Interrupt Link [ALKB] (IRQs 21, disabled)
ACPI: PCI Interrupt Link [ALKC] (IRQs 22, disabled)
ACPI: PCI Interrupt Link [ALKD] (IRQs 23, disabled)
```

Linux-Kernel: 2.6.0-test4-mm2: fdisk causes Oops

```
drivers/usb/core/usb.c: registered new driver usbfs
drivers/usb/core/usb.c: registered new driver hub
PCI: Probing PCI hardware
PCI: Using IRQ router VIA [1106/3177] at 0000:00:11.0
PCI->APIC IRQ transform: (B0,I10,P0) -> 18
PCI->APIC IRQ transform: (B0,I11,P0) -> 19
PCI->APIC IRQ transform: (B0,I15,P0) -> 19
PCI->APIC IRQ transform: (B0,I16,P0) -> 21
PCI->APIC IRQ transform: (B0,I16,P1) -> 21
PCI->APIC IRQ transform: (B0,I16,P2) -> 21
PCI->APIC IRQ transform: (B0,I16,P3) -> 21
PCI->APIC IRQ transform: (B0,I17,P0) -> 22
PCI->APIC IRQ transform: (B0,I17,P2) -> 22
PCI->APIC IRQ transform: (B0,I19,P0) -> 18
PCI->APIC IRQ transform: (B0,I20,P0) -> 16
PCI->APIC IRQ transform: (B1,I0,P0) -> 16
pty: 256 Unix98 ptys configured
Machine check exception polling timer started.
ikconfig 0.5 with /proc/ikconfig
highmem bounce pool size: 64 pages
PCI: Via IRQ fixup for 0000:00:10.0, from 7 to 5
PCI: Via IRQ fixup for 0000:00:10.1, from 6 to 5
PCI: Via IRQ fixup for 0000:00:10.2, from 10 to 5
ACPI: Power Button (FF) [PWRB]
ACPI: Processor [CPU0] (supports C1, 2 throttling states)
Real Time Clock Driver v1.11a
Linux agpgart interface v0.100 (c) Dave Jones
agpgart: Detected VIA Apollo Pro KT400 chipset
agpgart: Maximum main memory to use for agp memory: 941M
agpgart: AGP aperture is 256M @ 0xc0000000
Serial: 8250/16550 driver $Revision: 1.90 $ IRQ sharing disabled
ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
ttyS3 at I/O 0x2e8 (irq = 3) is a 16550A
3c59x: Donald Becker and others. www.scyld.com/network/vortex.html
0000:00:0a.0: 3Com PCI 3c905C Tornado at 0x9000. Vers LK1.1.19
Universal TUN/TAP device driver 1.5 (C)1999-2002 Maxim Krasnyansky
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PDC20276: IDE controller at PCI slot 0000:00:0f.0
PDC20276: chipset revision 1
PDC20276: 100% native mode on irq 19
   ide2: BM-DMA at 0xac00-0xac07, BIOS settings: hde:pio, hdf:pio
   ide3: BM-DMA at 0xac08-0xac0f, BIOS settings: hdg:pio, hdh:pio
hdg: QUANTUM SIROCCO1700A, ATA DISK drive
PM: Adding info for No Bus:ide3
hdh: SAMSUNG SV0322A, ATA DISK drive
Using anticipatory scheduling elevator
ide3 at 0xa400-0xa407,0xa802 on irq 19
PM: Adding info for ide:3.0
PM: Adding info for ide:3.1
VP_IDE: IDE controller at PCI slot 0000:00:11.1
```

Linux-Kernel: 2.6.0-test4-mm2: fdisk causes Oops

```
VP_IDE: chipset revision 6
VP_IDE: not 100% native mode: will probe irqs later
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
VP_IDE: VIA vt8235 (rev 00) IDE UDMA133 controller on pci0000:00:11.1
  ide0: BM-DMA at 0xbc00-0xbc07, BIOS settings: hda:DMA, hdb:pio
  ide1: BM-DMA at 0xbc08-0xbc0f, BIOS settings: hdc:DMA, hdd:pio
hda: WDC WD800JB-00ETA0, ATA DISK drive
PM: Adding info for No Bus:ide0
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
PM: Adding info for ide:0.0
hdc: Pioneer DVD-ROM ATAPIModel DVD-113 0114, ATAPI CD/DVD-ROM drive
PM: Adding info for No Bus:ide1
ide1 at 0x170-0x177,0x376 on irq 15
PM: Adding info for ide:1.0
hdg: max request size: 128KiB
hdg: 3335472 sectors (1707 MB) w/75KiB Cache, CHS=3309/16/63, DMA
  hdg: hdg1 hdg2
hdh: max request size: 128KiB
hdh: 6250608 sectors (3200 MB) w/478KiB Cache, CHS=11024/9/63, UDMA(33)
  hdh:
hda: max request size: 1024KiB
hda: 156301488 sectors (80026 MB) w/8192KiB Cache, CHS=16383/255/63, UDMA(100)
  hda: hda1 hda2
drivers/usb/host/uhci-hcd.c: USB Universal Host Controller Interface driver v2.1
uhci-hcd 0000:00:10.0: UHCI Host Controller
uhci-hcd 0000:00:10.0: irq 21, io base 0000b000
uhci-hcd 0000:00:10.0: new USB bus registered, assigned bus number 1
PM: Adding info for usb:usb1
hub 1-0:0: USB hub found
hub 1-0:0: 2 ports detected
PM: Adding info for usb:1-0:0
uhci-hcd 0000:00:10.1: UHCI Host Controller
uhci-hcd 0000:00:10.1: irq 21, io base 0000b400
uhci-hcd 0000:00:10.1: new USB bus registered, assigned bus number 2
PM: Adding info for usb:usb2
hub 2-0:0: USB hub found
hub 2-0:0: 2 ports detected
PM: Adding info for usb:2-0:0
uhci-hcd 0000:00:10.2: UHCI Host Controller
uhci-hcd 0000:00:10.2: irq 21, io base 0000b800
uhci-hcd 0000:00:10.2: new USB bus registered, assigned bus number 3
PM: Adding info for usb:usb3
hub 3-0:0: USB hub found
hub 3-0:0: 2 ports detected
PM: Adding info for usb:3-0:0
drivers/usb/core/usb.c: registered new driver hiddev
drivers/usb/core/usb.c: registered new driver hid
drivers/usb/input/hid-core.c: v2.0:USB HID core driver
mice: PS/2 mouse device common for all mice
serio: i8042 AUX port at 0x60,0x64 irq 12
input: AT Set 2 keyboard on isa0060/serio0
```

Linux-Kernel: 2.6.0-test4-mm2: fdisk causes Oops

```
serio: i8042 KBD port at 0x60,0x64 irq 1
i2c /dev entries driver module version 2.7.0 (20021208)
Advanced Linux Sound Architecture Driver Version 0.9.6 (Wed Aug 20 20:27:13 2003 UTC).
request_module: failed /sbin/modprobe -- snd-card-0. error = -16
ALSA device list:
 #0: Sound Blaster Live! (rev.7) at 0x9400, irq 19
NET4: Linux TCP/IP 1.0 for NET4.0
IP: routing cache hash table of 8192 buckets, 64Kbytes
TCP: Hash tables configured (established 262144 bind 65536)
ip_contrack version 2.1 (8191 buckets, 65528 max) - 160 bytes per contrack
ip_tables: (C) 2000-2002 Netfilter core team
ipt_recent v0.3.1: Stephen Frost <sfrost@snowman.net>. http://snowman.net/projects/ipt\_recent/
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
BIOS EDD facility v0.09 2003-Jan-22, 3 devices found
ACPI: (supports S0 S3 S4 S5)
EXT3-fs: INFO: recovery required on readonly filesystem.
EXT3-fs: write access will be enabled during recovery.
kjournald starting. Commit interval 5 seconds
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
VFS: Mounted root (ext3 filesystem) readonly.
Freeing unused kernel memory: 368k freed
hub 1-0:0: debounce: port 2: delay 100ms stable 4 status 0x301
hub 1-0:0: new USB device on port 2, assigned address 2
PM: Adding info for usb:1-2
EXT3 FS on hda2, internal journal
ttyS1: LSR safety check engaged!
ttyS1: LSR safety check engaged!
drivers/usb/input/hid-core.c: ctrl urb status -104 received
drivers/usb/input/hid-core.c: timeout initializing reports

input: USB HID v1.00 Mouse [Logitech Inc. iFeel Mouse ] on usb-0000:00:10.0-2
PM: Adding info for usb:1-2:0
hub 3-0:0: debounce: port 2: delay 100ms stable 4 status 0x101
hub 3-0:0: new USB device on port 2, assigned address 2
PM: Adding info for usb:3-2
hub 3-2:0: USB hub found
hub 3-2:0: 3 ports detected
PM: Adding info for usb:3-2:0
IPv6 v0.8 for NET4.0
IPv6 over IPv4 tunneling driver
hub 3-2:0: debounce: port 1: delay 100ms stable 4 status 0x101
hub 3-2:0: new USB device on port 1, assigned address 3
PM: Adding info for usb:3-2.1
input: USB HID v1.00 Keyboard [Chicony PFU-65 USB Keyboard] on usb-0000:00:10.2-2.1
PM: Adding info for usb:3-2.1:0
hub 2-0:0: debounce: port 2: delay 100ms stable 4 status 0x101
hub 2-0:0: new USB device on port 2, assigned address 2
PM: Adding info for usb:2-2
PM: Adding info for usb:2-2:0
```

Linux-Kernel: 2.6.0-test4-mm2: fdisk causes Oops

Unable to handle kernel NULL pointer dereference at virtual address 00000000

printing eip:

c021a1fd

*pde = 00000000

Oops: 0000 [#1]

PREEMPT

CPU: 0

EIP: 0060:[<c021a1fd>] Not tainted VLI

EFLAGS: 00010246

EIP is at generic_ide_ioctl+0x30d/0x7a0

eax: 00000000 ebx: bffffb68 ecx: f7ff1040 edx: 00000000

esi: bffffb60 edi: 00000ced ebp: f7577f68 esp: f7577f38

ds: 007b es: 007b ss: 0068

Process fdisk (pid: 398, threadinfo=f7576000 task=f7628670)

Stack: c0326f5f 0000064e 00000000 000b2345 c043f4a8 f7577f68 401363a8 bffffb00

f7577fbc f7ff1040 bffffb60 f759d0fc f7577f90 c0202a90 f7ff1040 00000301

bffffb60 bffffb60 00002200 00000301 f76043c0 fffffe7 f7577fbc c016d5c4

Call Trace:

[<c0202a90>] blkdev_ioctl+0x90/0x3ca

[<c016d5c4>] sys_ioctl+0xf4/0x2b0

[<c02fe977>] syscall_call+0x7/0xb

Code: 00 00 c7 04 24 5f 6f 32 c0 e8 30 64 f0 ff 83 c3 04 83 c3 04 19 c0 39 5e 18 83 d8 00 85 c0 75 1a 8b 4d
08 31 c0 8b 75 10 8b 51 38 <8b> 12 89 56 04 31 d2 85 c0 0f 84 61 fd ff ff ba f2 ff ff ff e9

00:00.0 Host bridge: VIA Technologies, Inc. VT8377 [KT400 AGP] Host Bridge

00:01.0 PCI bridge: VIA Technologies, Inc. VT8235 PCI Bridge

00:0a.0 Ethernet controller: 3Com Corporation 3c905C-TX/TX-M [Tornado] (rev 6c)

00:0b.0 Multimedia audio controller: Creative Labs SB Live! EMU10k1 (rev 07)

00:0b.1 Input device controller: Creative Labs SB Live! MIDI/Game Port (rev 07)

00:0f.0 RAID bus controller: Promise Technology, Inc. PDC20276 IDE (rev 01)

00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)

00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)

00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)

00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)

00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge

00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B PIPC Bus Master IDE (rev 06)

00:11.5 Multimedia audio controller: VIA Technologies, Inc. VT8233 AC97 Audio Controller (rev 50)

00:13.0 Ethernet controller: Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+ (rev 10)

00:14.0 FireWire (IEEE 1394): VIA Technologies, Inc. IEEE 1394 Host Controller (rev 46)

01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 82)

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to majordomo@vger.kernel.org

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>