

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2007-05/msg13826.html>

- *From:* Cameron Schaus <cam@xxxxxxxx>
 - *Date:* Thu, 31 May 2007 11:12:37 -0600
-

Hello All,

I am seeing the following kernel assertion (BUG) trip whenever I run a set of RPM commands. It is 100% reproducible, and occurs on a machine running vmware.

The kernel is a FC5 2.6.20-1-2316 kernel recompiled to disable CONFIG_DEBUG_SPINLOCK and CONFIG_DEBUG_SPINLOCK_SLEEP.

Is this a kernel bug?

list_del corruption. next->prev should be c1308018, but was 00000001

-----[cut here]-----

kernel BUG at lib/list_debug.c:72!

invalid opcode: 0000 [#1]

SMP

last sysfs file: /block/loop4/dev

Modules linked in: loop ipt_REDIRECT iptable_nat nf_nat ipt_REJECT xt_tcpudp iptable_filter ip_tables

x_tables nf_conntrack_ftp nf_conntrack_ipv4 nf_conntrack nfnetlink bri

dge ipv6 dm_mirror dm_mod video sbs i2c_ec dock button battery asus_acpi backlight ac lp parport_pc

parport floppy ata_piix libata serio_raw pnet32 mii BusLogic scsi_mod i

2c_piix4 i2c_core pcspkr ide_cd cdrom ext3 jbd

CPU: 0

EIP: 0060:[<c04e990e>] Not tainted VLI

EFLAGS: 00210092 (2.6.20-1.2322wecansmp #1)

EIP is at list_del+0x42/0x5d

eax: 00000048 ebx: 00000001 ecx: 00200086 edx: 00200000

esi: c06c177c edi: 0000000a ebp: c06c0680 esp: e7775cbc

ds: 007b es: 007b ss: 0068

Process rpm (pid: 2357, ti=e7775000 task=ea0b96f0 task.ti=e7775000)

Stack: c0679633 c1308018 00000001 c1308018 c0455fad 00000000 c1308000 c06c0680

00200246 c06c0700 00000013 c04567bf 00000002 00000044 00000000 00000002

00000000 000200d2 c06c2bb0 00000000 f7d2c400 0000001f 00000001 00000000

Call Trace:

[<c0455fad>] __rmqueue+0x32/0xa2

[<c04567bf>] get_page_from_freelist+0xfe/0x2a6

[<c04569c0>] __alloc_pages+0x59/0x29b

[<c0452686>] find_lock_page+0x1a/0x77

[<c045395d>] generic_file_buffered_write+0x198/0x5f8

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

```
[<c042a5b8>] current_fs_time+0x4f/0x5b
[<c045429e>] __generic_file_aio_write_nolock+0x4e1/0x55a
[<c04048cf>] common_interrupt+0x23/0x28
[<c045436c>] generic_file_aio_write+0x55/0xb3
[<f887bfdc>] ext3_file_write+0x24/0x8f [ext3]
[<c046ef49>] do_sync_write+0xc7/0x10a
[<c0437435>] autoremove_wake_function+0x0/0x35
[<c0461974>] do_mmap_pgoff+0x59a/0x702
[<c061bda8>] do_page_fault+0x338/0x5eb
[<c046ee82>] do_sync_write+0x0/0x10a
[<c046f788>] vfs_write+0xa8/0x154
[<c046fd97>] sys_write+0x41/0x67
[<c0403f34>] syscall_call+0x7/0xb
```

```
=====
Code: 24 e5 95 67 c0 e8 c6 d4 f3 ff 0f 0b eb fe 8b 10 8b 5a 04 39 c3 74 18 89 5c 24 08 89 44 24 04 c7 04 24
33 96 67 c0 e8 a5 d4 f3 ff <0f> 0b eb fe 89 4a 04 89 11 c7 40 04
00 02 20 00 c7 00 00 01 10
EIP: [<c04e990e>] list_del+0x42/0x5d SS:ESP 0068:e7775cbc
```

Dmesg:

Linux version 2.6.20-1.2322wecansmp (root@vegas) (gcc version 4.1.1 20070105 (Red Hat 4.1.1-51)) #1
SMP Tue May 29 15:50:29 MDT 2007

BIOS-provided physical RAM map:

sanitize start

sanitize end

copy_e820_map() start: 0000000000000000 size: 000000000009f800 end: 000000000009f800 type: 1

copy_e820_map() type is E820_RAM

copy_e820_map() start: 000000000009f800 size: 0000000000008000 end: 00000000000a0000 type: 2

copy_e820_map() start: 00000000000dc000 size: 0000000000240000 end: 0000000001000000 type: 2

copy_e820_map() start: 0000000001000000 size: 000000003e5f0000 end: 000000003e6f0000 type: 1

copy_e820_map() type is E820_RAM

copy_e820_map() start: 000000003e6f0000 size: 00000000000f0000 end: 000000003e6ff000 type: 3

copy_e820_map() start: 000000003e6ff000 size: 0000000000010000 end: 000000003e700000 type: 4

copy_e820_map() start: 000000003e700000 size: 0000000001000000 end: 000000003e800000 type: 1

copy_e820_map() type is E820_RAM

copy_e820_map() start: 00000000fec00000 size: 0000000000100000 end: 00000000fec10000 type: 2

copy_e820_map() start: 00000000fee00000 size: 0000000000010000 end: 00000000fee01000 type: 2

copy_e820_map() start: 00000000ffe00000 size: 0000000000200000 end: 0000000100000000 type: 2

BIOS-e820: 0000000000000000 - 000000000009f800 (usable)

BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)

BIOS-e820: 00000000000dc000 - 0000000000100000 (reserved)

BIOS-e820: 0000000000100000 - 000000003e6f0000 (usable)

BIOS-e820: 000000003e6f0000 - 000000003e6ff000 (ACPI data)

BIOS-e820: 000000003e6ff000 - 000000003e700000 (ACPI NVS)

BIOS-e820: 000000003e700000 - 000000003e800000 (usable)

BIOS-e820: 00000000fec00000 - 00000000fec10000 (reserved)

BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)

BIOS-e820: 00000000ffe00000 - 0000000100000000 (reserved)

104MB HIGHMEM available.

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

896MB LOWMEM available.
found SMP MP-table at 000f6ce0
Using x86 segment limits to approximate NX protection
Entering add_active_range(0, 0, 256000) 0 entries of 256 used
Zone PFN ranges:
DMA 0 -> 4096
Normal 4096 -> 229376
HighMem 229376 -> 256000
early_node_map[1] active PFN ranges
0: 0 -> 256000
On node 0 totalpages: 256000
DMA zone: 32 pages used for memmap
DMA zone: 0 pages reserved
DMA zone: 4064 pages, LIFO batch:0
Normal zone: 1760 pages used for memmap
Normal zone: 223520 pages, LIFO batch:31
HighMem zone: 208 pages used for memmap
HighMem zone: 26416 pages, LIFO batch:7
DMI present.
Using APIC driver default
ACPI: RSDP (v000 PTLTD) @ 0x000f6c70
ACPI: RSDT (v001 PTLTD RSDT 0x06040000 LTP 0x00000000) @ 0x3e6fab74
ACPI: FADT (v001 INTEL 440BX 0x06040000 PTL 0x000f4240) @ 0x3e6fef14
ACPI: MADT (v001 PTLTD APIC 0x06040000 LTP 0x00000000) @ 0x3e6fef88
ACPI: BOOT (v001 PTLTD \$SBFTBLS\$ 0x06040000 LTP 0x00000001) @ 0x3e6fefd8
ACPI: DSDT (v001 PTLTD Custom 0x06040000 MSFT 0x0100000d) @ 0x00000000
ACPI: PM-Timer IO Port: 0x1008
ACPI: Local APIC address 0xfe00000
ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Processor #0 15:2 APIC version 17
ACPI: LAPIC_NMI (acpi_id[0x00] high edge lint[0x1])
ACPI: IOAPIC (id[0x01] address[0xfec00000] gsi_base[0])
IOAPIC[0]: apic_id 1, version 17, address 0xfec00000, GSI 0-23
ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 high edge)
ACPI: IRQ0 used by override.
ACPI: IRQ2 used by override.
ACPI: IRQ9 used by override.
Enabling APIC mode: Flat. Using 1 I/O APICs
Using ACPI (MADT) for SMP configuration information
Allocating PCI resources starting at 40000000 (gap: 3e800000:c0400000)
Detected 2790.864 MHz processor.
Built 1 zonelists. Total pages: 254000
Kernel command line: ro root=LABEL=/ console=ttyS0,9600 console=tty1
mapped APIC to fffd000 (fee00000)
mapped IOAPIC to fffc000 (fec00000)
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Initializing CPU#0
CPU 0 irqstacks, hard=c0764000 soft=c0744000
PID hash table entries: 4096 (order: 12, 16384 bytes)
Console: colour VGA+ 80x25

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

Dentry cache hash table entries: 131072 (order: 7, 524288 bytes)
Inode-cache hash table entries: 65536 (order: 6, 262144 bytes)
Memory: 1009428k/1024000k available (2165k kernel code, 13808k reserved, 899k data, 236k init, 106432k highmem)
virtual kernel memory layout:
fixmap : 0xffc56000 – 0xfffff000 (3748 kB)
pkmap : 0xffa00000 – 0xffc00000 (2048 kB)
vmalloc : 0xf8800000 – 0xff9fe000 (113 MB)
lowmem : 0xc0000000 – 0xf8000000 (896 MB)
.init : 0xc0704000 – 0xc073f000 (236 kB)
.data : 0xc061d6e2 – 0xc06fe494 (899 kB)
.text : 0xc0400000 – 0xc061d6e2 (2165 kB)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Calibrating delay using timer specific routine.. 5589.06 BogoMIPS (lpj=2794534)
Security Framework v1.0.0 initialized
SELinux: Initializing.
SELinux: Starting in permissive mode
selinux_register_security: Registering secondary module capability
Capability LSM initialized as secondary
Mount-cache hash table entries: 512
CPU: After generic identify, caps: 0febfbff 00000000 00000000 00000000 00000000 00000000
CPU: Trace cache: 12K uops, L1 D cache: 8K
CPU: L2 cache: 512K
CPU: After all inits, caps: 0feb3ff 00000000 00000000 00003080 00000000 00000000 00000000
Intel machine check architecture supported.
Intel machine check reporting enabled on CPU#0.
Checking 'hlt' instruction... OK.
SMP alternatives: switching to UP code
Freeing SMP alternatives: 14k freed
ACPI: Core revision 20060707
CPU0: Intel(R) Pentium(R) 4 CPU 2.80GHz stepping 08
Total of 1 processors activated (5589.06 BogoMIPS).
ENABLING IO-APIC IRQs
..TIMER: vector=0x31 apic1=0 pin1=2 apic2=-1 pin2=-1
Brought up 1 CPUs
sizeof(vma)=88 bytes
sizeof(page)=32 bytes
sizeof(inode)=336 bytes
sizeof(dentry)=132 bytes
sizeof(ext3inode)=488 bytes
sizeof(buffer_head)=56 bytes
sizeof(skbuff)=176 bytes
sizeof(task_struct)=1408 bytes
NET: Registered protocol family 16
ACPI: bus type pci registered
PCI: PCI BIOS revision 2.10 entry at 0xfd9a0, last bus=1
PCI: Using configuration type 1
Setting up standard PCI resources
ACPI: Interpreter enabled
ACPI: Using IOAPIC for interrupt routing
ACPI: PCI Root Bridge [PCI0] (0000:00)

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

PCI: Probing PCI hardware (bus 00)
0000:00:07.1: cannot adjust BAR0 (not I/O)
0000:00:07.1: cannot adjust BAR1 (not I/O)
0000:00:07.1: cannot adjust BAR2 (not I/O)
0000:00:07.1: cannot adjust BAR3 (not I/O)
PCI quirk: region 1000-103f claimed by PIIX4 ACPI
PCI quirk: region 1040-104f claimed by PIIX4 SMB
Boot video device is 0000:00:0f.0
ACPI: PCI Interrupt Routing Table [_SB_.PCI0._PRT]
ACPI: PCI Interrupt Link [LNKA] (IRQs 3 4 5 6 7 9 10 11 14 15) *0, disabled.
ACPI: PCI Interrupt Link [LNKB] (IRQs 3 4 5 6 7 9 10 *11 14 15)
ACPI: PCI Interrupt Link [LNKC] (IRQs 3 4 5 6 7 *9 10 11 14 15)
ACPI: PCI Interrupt Link [LNKD] (IRQs 3 4 5 6 7 9 10 11 14 15) *0, disabled.
Linux Plug and Play Support v0.97 (c) Adam Belay
pnp: PnP ACPI init
pnp: PnP ACPI: found 12 devices
usbcore: registered new interface driver usbfs
usbcore: registered new interface driver hub
usbcore: registered new device driver usb
PCI: Using ACPI for IRQ routing
PCI: If a device doesn't work, try "pci=routeirq". If it helps, post a report
NetLabel: Initializing
NetLabel: domain hash size = 128
NetLabel: protocols = UNLABELED CIPSOv4
NetLabel: unlabeled traffic allowed by default
PCI: Bridge: 0000:00:01.0
IO window: disabled.
MEM window: disabled.
PREFETCH window: disabled.
PCI: Setting latency timer of device 0000:00:01.0 to 64
NET: Registered protocol family 2
IP route cache hash table entries: 32768 (order: 5, 131072 bytes)
TCP established hash table entries: 131072 (order: 8, 1048576 bytes)
TCP bind hash table entries: 65536 (order: 7, 524288 bytes)
TCP: Hash tables configured (established 131072 bind 65536)
TCP reno registered
checking if image is initramfs... it is
Freeing initrd memory: 904k freed
Simple Boot Flag at 0x36 set to 0x1
apm: BIOS version 1.2 Flags 0x03 (Driver version 1.16ac)
apm: overridden by ACPI.
audit: initializing netlink socket (disabled)
audit(1180609718.255:1): initialized
highmem bounce pool size: 64 pages
Total HugeTLB memory allocated, 0
VFS: Disk quotas dquot_6.5.1
Dquot-cache hash table entries: 1024 (order 0, 4096 bytes)
SELinux: Registering netfilter hooks
ksign: Installing public key data
Loading keyring
- Added public key FA613C3CC4C4EF16

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

– User ID: Red Hat, Inc. (Kernel Module GPG key)
io scheduler noop registered
io scheduler anticipatory registered
io scheduler deadline registered
io scheduler cfq registered (default)
Limiting direct PCI/PCI transfers.
pci_hotplug: PCI Hot Plug PCI Core version: 0.5
ACPI: Processor [CPU0] (supports 8 throttling states)
ACPI Exception (acpi_processor-0677): AE_NOT_FOUND, Processor Device is not present [20060707]
ACPI Exception (acpi_processor-0677): AE_NOT_FOUND, Processor Device is not present [20060707]
ACPI Exception (acpi_processor-0677): AE_NOT_FOUND, Processor Device is not present [20060707]
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Real Time Clock Driver v1.12ac
Non-volatile memory driver v1.2
Linux agpgart interface v0.101 (c) Dave Jones
agpgart: Detected an Intel 440BX Chipset.
agpgart: AGP aperture is 64M @ 0xec000000
Serial: 8250/16550 driver \$Revision: 1.90 \$ 4 ports, IRQ sharing enabled
serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
serial8250: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
00:09: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
00:0a: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
RAMDISK driver initialized: 16 RAM disks of 16384K size 4096 blocksize
input: Macintosh mouse button emulation as /class/input/input0
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller at PCI slot 0000:00:07.1
PIIX4: chipset revision 1
PIIX4: not 100% native mode: will probe irqs later
ide0: BM-DMA at 0x1050-0x1057, BIOS settings: hda:DMA, hdb:pio
ide1: BM-DMA at 0x1058-0x105f, BIOS settings: hdc:DMA, hdd:pio
Probing IDE interface ide0...
hda: VMware Virtual IDE Hard Drive, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
Probing IDE interface ide1...
hdc: VMware Virtual IDE CDROM Drive, ATAPI CD/DVD-ROM drive
ide1 at 0x170-0x177,0x376 on irq 15
hda: max request size: 128KiB
hda: 8388608 sectors (4294 MB) w/32KiB Cache, CHS=8322/16/63, UDMA(33)
hda: hda1
ide-floppy driver 0.99.newide
usbcore: registered new interface driver libusual
usbcore: registered new interface driver hiddev
usbcore: registered new interface driver usbhid
drivers/usb/input/hid-core.c: v2.6:USB HID core driver
PNP: PS/2 Controller [PNP0303:KBC,PNP0f13:MOUS] at 0x60,0x64 irq 1,12
serio: i8042 KBD port at 0x60,0x64 irq 1
serio: i8042 AUX port at 0x60,0x64 irq 12
mice: PS/2 mouse device common for all mice
input: AT Translated Set 2 keyboard as /class/input/input1

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

TCP bic registered
Initializing XFRM netlink socket
NET: Registered protocol family 1
NET: Registered protocol family 17
Using IPI No-Shortcut mode
ACPI: (supports<6>Time: tsc clocksource has been installed.
S0 S1 S5)
Freeing unused kernel memory: 236k freed
Write protecting the kernel read-only data: 594k
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: hda1: orphan cleanup on readonly fs
ext3_orphan_cleanup: deleting unreferenced inode 951849
ext3_orphan_cleanup: deleting unreferenced inode 852950
ext3_orphan_cleanup: deleting unreferenced inode 852943
ext3_orphan_cleanup: deleting unreferenced inode 852937
ext3_orphan_cleanup: deleting unreferenced inode 852928
ext3_orphan_cleanup: deleting unreferenced inode 557065
ext3_orphan_cleanup: deleting unreferenced inode 557064
ext3_orphan_cleanup: deleting unreferenced inode 557063
ext3_orphan_cleanup: deleting unreferenced inode 557060
ext3_orphan_cleanup: deleting unreferenced inode 557059
EXT3-fs: hda1: 10 orphan inodes deleted
EXT3-fs: recovery complete.
input: ImPS/2 Generic Wheel Mouse as /class/input/input2
EXT3-fs: mounted filesystem with ordered data mode.
SELinux: Disabled at runtime.
SELinux: Unregistering netfilter hooks
audit(1180609722.615:2): selinux=0 auid=4294967295
piix4_smbus 0000:00:07.3: Found 0000:00:07.3 device
piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!
hdc: ATAPI 1X CD-ROM drive, 32kB Cache, UDMA(33)
Uniform CD-ROM driver Revision: 3.20
pcnet32.c:v1.33-NAPI 27.Jun.2006 tsbogend@xxxxxxxxxxxxxxxxx
ACPI: PCI Interrupt 0000:00:11.0[A] -> GSI 18 (level, low) -> IRQ 16
pcnet32: PCnet/PCI II 79C970A at 0x1080, 00 0c 29 57 51 02 assigned IRQ 16.
eth0: registered as PCnet/PCI II 79C970A
pcnet32: 1 cards_found.
input: PC Speaker as /class/input/input3
SCSI subsystem initialized
ACPI: PCI Interrupt 0000:00:10.0[A] -> GSI 17 (level, low) -> IRQ 17
scsi: ***** BusLogic SCSI Driver Version 2.1.16 of 18 July 2002 *****
scsi: Copyright 1995-1998 by Leonard N. Zubkoff <lnz@xxxxxxxxxxxxxxxx>
scsi0: Configuring BusLogic Model BT-958 PCI Wide Ultra SCSI Host Adapter
scsi0: Firmware Version: 5.07B, I/O Address: 0x1060, IRQ Channel: 17/Level
scsi0: PCI Bus: 0, Device: 16, Address: 0xE8800000, Host Adapter SCSI ID: 7
scsi0: Parity Checking: Enabled, Extended Translation: Enabled
scsi0: Synchronous Negotiation: Ultra, Wide Negotiation: Enabled
scsi0: Disconnect/Reconnect: Enabled, Tagged Queuing: Enabled
scsi0: Scatter/Gather Limit: 128 of 8192 segments, Mailboxes: 211

Kernel assertion (BUG) on 2.6.20-1-2316 FC5

scsi0: Driver Queue Depth: 211, Host Adapter Queue Depth: 192
scsi0: Tagged Queue Depth: Automatic, Untagged Queue Depth: 3
scsi0: *** BusLogic BT-958 Initialized Successfully ***
scsi0 : BusLogic BT-958
libata version 2.00 loaded.
Floppy drive(s): fd0 is 1.44M
FDC 0 is a post-1991 82077
parport: PnPBIOS parport detected.
parport0: PC-style at 0x378, irq 7 [PCSPP,TRISTATE]
lp0: using parport0 (interrupt-driven).
lp0: console ready
ACPI: AC Adapter [ACAD] (on-line)
input: Power Button (FF) as /class/input/input4
ACPI: Power Button (FF) [PWRF]
No dock devices found.
ibm_acpi: ec object not found
md: Autodetecting RAID arrays.
md: autorun ...
md: ... autorun DONE.
device-mapper: ioctl: 4.11.0-ioctl (2006-10-12) initialised: dm-devel@xxxxxxxxxx
EXT3 FS on hda1, internal journal

—
To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to majordomo@xxxxxxxxxxxxxxxxxx
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>