

Re: PROBLEM: kernel BUG at mm/rmap.c:522!

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2007-04/msg04790.html>

- *From:* Hugh Dickins <hugh@xxxxxxxxxxxx>
 - *Date:* Fri, 13 Apr 2007 13:43:39 +0100 (BST)
-

On Fri, 13 Apr 2007, Francesco Ricci wrote:

[7.7.] Other information that might be relevant to the problem (please look in /proc and include all information that you think to be relevant):

Thanks for your report, and for your patience in supplying all that scarcely relevant info you were asked for.

from dmesg:

```
Apr 13 11:31:35 localhost kernel: Bad pte = 461b43d4, process = ???,
vm_flags = 75, vaddr = b7868000
```

Oh dear, one of your page tables has got corrupted, the page table entry for virtual address b7868000 contains 461b43d4 – nonsense.

```
Apr 13 11:31:35 localhost kernel: [<c014b0ea>] vm_normal_page+0x3e/0x53
Apr 13 11:31:35 localhost kernel: [<c014b6fa>] unmap_vmas+0x183/0x4af
Apr 13 11:31:35 localhost kernel: [<c014de31>] exit_mmap+0x6a/0xd7
Apr 13 11:31:35 localhost kernel: [<c011b217>] mmput+0x20/0x76
Apr 13 11:31:35 localhost kernel: [<c011fa05>] do_exit+0x193/0x71b
Apr 13 11:31:35 localhost kernel: [<c0120003>] sys_exit_group+0x0/0xd
Apr 13 11:31:35 localhost kernel: [<c0127a6d>]
get_signal_to_deliver+0x395/0x3bc
Apr 13 11:31:35 localhost kernel: [<c01023a6>] do_notify_resume+0x71/0x5d7
Apr 13 11:31:35 localhost kernel: [<c0117778>]
default_wake_function+0x0/0xc
Apr 13 11:31:35 localhost kernel: [<c0124657>] do_gettimeofday+0x31/0xce
Apr 13 11:31:35 localhost kernel: [<c0131ffc>] sys_futex+0xdc/0xf1
Apr 13 11:31:35 localhost kernel: [<c0102d0a>] work_notifysig+0x13/0x19
Apr 13 11:31:35 localhost kernel: -----[ cut here ]-----
Apr 13 11:31:35 localhost kernel: kernel BUG at mm/rmap.c:522!
Apr 13 11:31:35 localhost kernel: invalid opcode: 0000 [#1]
```

Re: PROBLEM: kernel BUG at mm/rmap.c:522!

```
Apr 13 11:31:35 localhost kernel: SMP
Apr 13 11:31:35 localhost kernel: Modules linked in: smbfs ext3 jbd
mbcache mga drm ppdev lp button ac battery ipv6 fuse dm_snapshot dm_mirror
dm_mod loop tsdev snd_via82xx gameport snd_ac97_codec snd_ac97_bus
snd_pcm_oss snd_mixer_oss snd_pcm snd_page_alloc snd_mpu401_uart
snd_seq_dummy snd_seq_oss snd_seq_midi snd_seq_midi_event snd_seq
i2c_viapro i2c_core snd_timer snd_rawmidi snd_seq_device via_agp
parport_pc parport via_ircc psmouse serio_raw floppy snd soundcore pcpkr
rtc agpgart shpchp pci_hotplug irda crc_ccitt evdev reiserfs ide_cd cdrom
ide_disk generic via_rhine mii ehci_hcd uhci_hcd via82cxxx ide_core
usbcore thermal processor fan
Apr 13 11:31:35 localhost kernel: CPU: 0
Apr 13 11:31:35 localhost kernel: EIP: 0060:[<c01506c9>] Not tainted
VLI
Apr 13 11:31:35 localhost kernel: EFLAGS: 00210286 (2.6.18-4-686 #1)
Apr 13 11:31:35 localhost kernel: EIP is at page_remove_rmap+0x14/0x2d
Apr 13 11:31:35 localhost kernel: eax: ffffffff ebx: c1000000 ecx:
c1000000 edx: 00000000
Apr 13 11:31:35 localhost kernel: esi: b7869000 edi: 00000000 ebp:
d08011a4 esp: c9be9e14
Apr 13 11:31:35 localhost kernel: ds: 007b es: 007b ss: 0068
Apr 13 11:31:35 localhost kernel: Process iceape-bin (pid: 20500,
ti=c9be8000 task=c2128aa0 task.ti=c9be8000)
Apr 13 11:31:35 localhost kernel: Stack: c014b7d5 00000000 df10d278
c9be9e7c 00000000 00000001 b7884000 c4bc7b78
Apr 13 11:31:35 localhost kernel: e80fbe40 c16058a0 00000000
ffffffe2 c121002c c4bc7b78 0011ed07 b7884000
Apr 13 11:31:35 localhost kernel: 00000000 c9be9e7c df4c7710
e80fbe40 c9be9eb8 c014de31 ffffffff c9be9e78
```

And the next page table entry, for virtual address b7869000, has also got corrupted: I'm rather guessing, but I believe the c1000000 implies it's looking at pfn 0, so the page table entry in question would be that 00000001 seen on the stack (1 for present).

That by itself would suggest a single-bit error, which would point you to running memtest86 overnight to check your RAM. Worth a try.

But the 461b43d4 before it suggests corruption from elsewhere in the kernel: sorry, I've no clue on that. Just wait and see if this happens again, and whether a pattern emerges – unless someone else can suggest something better.

Hugh

```
Apr 13 11:31:35 localhost kernel: Call Trace:
Apr 13 11:31:35 localhost kernel: [<c014b7d5>] unmap_vmas+0x25e/0x4af
Apr 13 11:31:35 localhost kernel: [<c014de31>] exit_mmap+0x6a/0xd7
Apr 13 11:31:35 localhost kernel: [<c011b217>] mmput+0x20/0x76
```

Re: PROBLEM: kernel BUG at mm/rmap.c:522!

Re: PROBLEM: kernel BUG at mm/rmap.c:522!

```
Apr 13 11:31:35 localhost kernel: [<c011fa05>] do_exit+0x193/0x71b
Apr 13 11:31:35 localhost kernel: [<c0120003>] sys_exit_group+0x0/0xd
Apr 13 11:31:35 localhost kernel: [<c0127a6d>]
get_signal_to_deliver+0x395/0x3bc
Apr 13 11:31:35 localhost kernel: [<c01023a6>] do_notify_resume+0x71/0x5d7
Apr 13 11:31:35 localhost kernel: [<c0117778>]
default_wake_function+0x0/0xc
Apr 13 11:31:35 localhost kernel: [<c0124657>] do_gettimeofday+0x31/0xce
Apr 13 11:31:35 localhost kernel: [<c0131ffc>] sys_futex+0xdc/0xf1
Apr 13 11:31:35 localhost kernel: [<c0102d0a>] work_notifysig+0x13/0x19
Apr 13 11:31:35 localhost kernel: Code: ff ff 85 c0 89 c6 75 c9 b0 01 86
43 28 83 c4 20 89 e8 5b 5e 5f 5d c3 89 c1 90 83 40 08 ff 0f 98 c0 84 c0 74
1e 8b 41 08 40 79 08 <0f> 0b 0a 02 40 ab 29 c0 8b 51 10 89 c8 83 f2 01 83
e2 01 e9 97
Apr 13 11:31:35 localhost kernel: EIP: [<c01506c9>]
page_remove_rmap+0x14/0x2d SS:ESP 0068:c9be9e14
Apr 13 11:31:35 localhost kernel: <1>Fixing recursive fault but reboot is
needed!
```

—

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