

## 2.6.3: NULL pointer deref in get\_disk()

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-02/7619.html>

---

**From:** Calum Mackay ([calum.mackay\\_at\\_cdmnet.org](mailto:calum.mackay_at_cdmnet.org))

**Date:** 02/28/04

Date: Sat, 28 Feb 2004 11:21:02 +0000  
To: linux-kernel@vger.kernel.org

I've recently started seeing the following on every attempt to mount a CompactFlash card – with a VFAT fs on it.

I am pretty sure that I've been able to mount this CF card previously, with the same 2.6.3 kernel, and in fact even during this boot uptime.

any thoughts?

cheers,  
c.

```
diz $ mount -V
mount: mount-2.12
diz $ uname -a
Linux diz 2.6.3 #16 Fri Feb 20 13:48:22 GMT 2004 i686 GNU/Linux
```

```
Feb 28 11:11:18 cdmnet kernel: <1>Unable to handle kernel NULL pointer
dereference at virtual address 00000804
Feb 28 11:11:18 cdmnet kernel: printing eip:
Feb 28 11:11:18 cdmnet kernel: c01e94a2
Feb 28 11:11:18 cdmnet kernel: *pde = 00000000
Feb 28 11:11:18 cdmnet kernel: Oops: 0000 [#1831]
Feb 28 11:11:18 cdmnet kernel: CPU: 0
Feb 28 11:11:18 cdmnet kernel: EIP: 0060:[get_disk+18/168] Not tainted
Feb 28 11:11:18 cdmnet kernel: EFLAGS: 00210206
Feb 28 11:11:18 cdmnet kernel: EIP is at get_disk+0x12/0xa8
Feb 28 11:11:18 cdmnet kernel: eax: 000007f0 ebx: edd96a80 ecx:
00000008 edx: 00000001
Feb 28 11:11:18 cdmnet kernel: esi: 00000000 edi: edd96a80 ebp:
c01e8e2c esp: cf719c54Feb 28 11:11:18 cdmnet kernel: ds: 007b es:
007b ss: 0068
Feb 28 11:11:18 cdmnet kernel: Process mount (pid: 13879,
threadinfo=cf718000 task=e4190ce0)
Feb 28 11:11:18 cdmnet kernel: Stack: edd96a80 00000000 d1d3ef40
c01e8e42 edd96a80 c01e3bd7 00800001 edd96a80
Feb 28 11:11:18 cdmnet kernel: cf718000 e60c1180 e60c1180
```

## Linux-Kernel: 2.6.3: NULL pointer deref in get\_disk()

```
00000001 0000000f c01e8ecd efd2c800 00800001
Feb 28 11:11:18 cdmnet kernel: cf719cc0 c0151c32 00800001
cf719cc0 00000000 e60c1180 cf719de0 00000001
Feb 28 11:11:18 cdmnet kernel: Call Trace:
Feb 28 11:11:18 cdmnet kernel: [exact_lock+10/32] exact_lock+0xa/0x20
Feb 28 11:11:19 cdmnet kernel: [kobj_lookup+199/444] kobj_lookup+0xc7/0x1bc
Feb 28 11:11:19 cdmnet kernel: [get_gendisk+21/44] get_gendisk+0x15/0x2c
Feb 28 11:11:19 cdmnet kernel: [do_open+70/988] do_open+0x46/0x3dc
Feb 28 11:11:19 cdmnet kernel: [blkdev_get+109/124] blkdev_get+0x6d/0x7c
Feb 28 11:11:19 cdmnet kernel: [open_bdev_excl+66/140]
open_bdev_excl+0x42/0x8c
Feb 28 11:11:19 cdmnet kernel: [get_sb_bdev+29/304] get_sb_bdev+0x1d/0x130
Feb 28 11:11:19 cdmnet kernel: [kmem_cache_alloc+47/56]
kmem_cache_alloc+0x2f/0x38
Feb 28 11:11:19 cdmnet kernel: [__crc_do_softirq+304176/2176560]
gcc2_compiled.+0x1f/0x24 [vfat]
Feb 28 11:11:19 cdmnet kernel: [__crc_do_softirq+304069/2176560]
vfat_fill_super+0x0/0x4c [vfat]
Feb 28 11:11:19 cdmnet kernel: [do_kern_mount+74/180]
do_kern_mount+0x4a/0xb4
Feb 28 11:11:19 cdmnet kernel: [do_add_mount+105/312]
do_add_mount+0x69/0x138
Feb 28 11:11:19 cdmnet kernel: [do_mount+354/380] do_mount+0x162/0x17c
Feb 28 11:11:19 cdmnet kernel: [copy_mount_options+128/248]
copy_mount_options+0x80/0xf8
Feb 28 11:11:19 cdmnet kernel: [sys_mount+167/276] sys_mount+0xa7/0x114
Feb 28 11:11:19 cdmnet kernel: [sysenter_past_esp+82/113]
sysenter_past_esp+0x52/0x71
Feb 28 11:11:19 cdmnet kernel:
Feb 28 11:11:19 cdmnet kernel: Code: 8b 70 14 85 f6 74 3b bb 01 00 00 00
b8 00 e0 ff ff 21 e0 ff
```

—  
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/>