
Subject: 2.6.24 repository with buggy scsi driver
Posted by [csurbhi](#) on Fri, 20 Feb 2009 12:14:41 GMT
[View Forum Message](#) <> [Reply to Message](#)

I have downloaded the linux kernel with openVZ support from the git source repository site <http://git.openvz.org/>.

I downloaded 2.6.24 and compiled it for a VmWare image. I have configured the disks as scsi! I tried booting the compiled version. I have configured the serial console so as to put the boot messages in a file. I can see that there is a bug in the scsi driver I googled for this and saw that its a reported bug and patched too. I would just like to bring this to notice, so that the patched kernel is uploaded

For your information I am pasting the stack trace and boot message which is relevant !!

Cheers,
Surbhi.

scsi0 : ioc0: LSI53C1030 B0, FwRev=00000000h, Ports=1, MaxQ=128, IRQ=16

BUG: unable to handle kernel paging request at virtual address fffff84

printing eip: c020550d *pde = 00426067 *pte = 00000000

Oops: 0002 [#1] SMP

Modules linked in: pcnet32 ehci_hcd uhci_hcd mii ata_piix usbcore mptspi mptscsih mptbase
scsi_transport_spi libata scsi_mod

Pid: 2139, comm: scsi_scan_0 Not tainted (2.6.24 #10 ovz008)

EIP: 0060:[<c020550d>] EFLAGS: 00010283 CPU: 0

EIP is at cfq_set_request+0x10d/0x360

EAX: 00000000 EBX: df811058 ECX: f7fb59c0 EDX: 00000000

ESI: df811000 EDI: 00000001 EBP: 00000005 ESP: df9f1ce4

DS: 007b ES: 007b FS: 00d8 GS: 0000 SS: 0068

Process scsi_scan_0 (pid: 2139, veid: 0, ti=df9f0000 task=df9f2c60 task.ti=df9f0000)

Stack: 00000010 00000010 f7fb59c0 df9a9000 00000000 df940200 df9f2c60 00000246

00000286 c0205400 df9a9000 00000004 00000000 c01fb06c df9a9000 f7fb59c0

c01ff05d c0198be5 c020cc75 00000008 df81f508 00000007 df81f508 00000000

Call Trace:

[<c0205400>] cfq_set_request+0x0/0x360

[<c01fb06c>] elv_set_request+0x1c/0x40

[<c01ff05d>] get_request+0x29d/0x320

[<c0198be5>] __slab_alloc+0x335/0x560

[<c020cc75>] vsnprintf+0x425/0x7b0

[<c01ffd5b>] get_request_wait+0x1b/0x1b0

[<f88308ee>] spi_target_match+0xe/0x80 [scsi_transport_spi]

[<f882f16d>] spi_host_match+0xd/0x70 [scsi_transport_spi]

[<c0270961>] attribute_container_add_device+0x61/0x130

[<c0270b50>] transport_setup_classdev+0x0/0x30

[<c01fff0c>] blk_get_request+0x1c/0x80

[<f885d8a6>] scsi_execute+0x36/0x110 [scsi_mod]

[<f885d9f9>] scsi_execute_req+0x79/0xf0 [scsi_mod]

[<f885e78a>] scsi_probe_and_add_lun+0x25a/0xbf0 [scsi_mod]

```
[<c02081ff>] kobject_get+0xf/0x20
[<c026ace0>] get_device+0x10/0x20
[<f885f4b3>] scsi_alloc_target+0x293/0x370 [scsi_mod]
[<f885f710>] __scsi_scan_target+0xe0/0x700 [scsi_mod]
[<c01203ab>] set_next_entity+0x2b/0x70
[<c0120443>] pick_next_task_fair+0x23/0x30
[<c014b844>] ub_slab_uncharge+0x34/0x50
[<f885fd89>] scsi_scan_channel+0x59/0xa0 [scsi_mod]
[<f885fe8d>] scsi_scan_host_selected+0xbd/0x180 [scsi_mod]
[<f885ffd0>] do_scan_async+0x0/0x150 [scsi_mod]
[<f885ffb>] do_scsi_scan_host+0x6f/0x80 [scsi_mod]
[<f885ffd0>] do_scan_async+0x0/0x150 [scsi_mod]
[<f885ffe1>] do_scan_async+0x11/0x150 [scsi_mod]
[<c01230a0>] complete+0x40/0x60
[<f885ffd0>] do_scan_async+0x0/0x150 [scsi_mod]
[<c0140049>] kthread+0x39/0x70
[<c0140010>] kthread+0x0/0x70
[<c0105737>] kernel_thread_helper+0x7/0x10
```

=====

Code: 24 0c 8b 82 20 01 00 00 8b 54 24 1c e8 7d cc 10 00 31 d2 8b 4c 24 08 89 71 58 89 59 5c
8b 43 54 8b 40 14 3d 80 00 00 00 74 3f 90 <ff> 40 84 31 d2 83 c4 24 89 d0 5b 5e 5f 5d c3 8d 74
26 00 8b 46

EIP: [<c020550d>] cfq_set_request+0x10d/0x360 SS:ESP 0068:df9f1ce4

---[end trace e2410052b7066c64]---