Subject: 2.6.24 bug report: problems with vzmigrate
Posted by Dietmar Maurer on Mon, 17 Mar 2008 11:29:44 GMT
View Forum Message <> Reply to Message

Unfortunately i am unable to reproduce that bug, but maybe it is
interesing for somebody anyways:

Unable to handle kernel NULL pointer dereference at 0000000000000000
RIP: [<0000000000000000>] _stext+0x7fdf7000/0x1a
PGD 2107fe067 PUD 21003b067 PMD 0
Oops: 0010 [1] PREEMPT SMP
CPU: 1
Modules linked in: nls_iso8859_1 nls_cp437 vfat kvm_intel kvm vzethdev
vznetdev simfs vzrst vzcpt tun vzdquota vzmon vzdev xt_tcpudp xt_length
ipt_ttl xt_tcpmss xt_TCPMSS iptable_mangle iptable_filter xt_multiport
xt_limit ipt_tos ipt_REJEC T ip_tables x_tables ipv6 sg bridge
dm_snapshot dm_mirror thermal psmouse e1000 evdev button e1000e
processor serio_raw floppy pcspkr dm_mod usbhid hid usb_stor age sd_mod
sr_mod ide_disk ide_generic ide_cd cdrom uhci_hcd ehci_hcd iTCO_wdt i
2c_i801 i2c_core generic ide_core ata_piix ata_generic libata shpchp
pci_hotplug aacraid scsi_mod isofs zlib_inflate msdos fat
Pid: 14529, comm: vzctl Not tainted 2.6.24 #1 ovz002
RIP: 0010:[<0000000000000000>] [<0000000000000000>]
_stext+0x7fdf7000/0x1a
RSP: 0018:ffff810214841d00 EFLAGS: 00010246
RAX: ffff810214841fd8 RBX: ffff810000000000 RCX: ffff810214841d58
RDX: 0000000000001000 RSI: ffff81010f8f1000 RDI: ffff8101ff6206c0
RBP: 00000000ffffffea R08: ffff8101e093b580 R09: ffff81021256d528
R10: ffff810212d1c400 R11: 0000000000000070 R12: ffff810211beb000
R13: ffff810211beb1d8 R14: ffff8101ff6206c0 R15: ffffffffffffffff
FS: 00002aeb65bafae0(0000) GS:ffff810215cba940(0000)
knlGS:0000000000000000
CS: 0010 DS: 0000 ES: 0000 CR0: 000000008005003b
CR2: 0000000000000000 CR3: 0000000202c2b000 CR4: 00000000000026e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
Process vzctl (pid: 14529, veid=0, threadinfo ffff810214840000, task
ffff810113c 836a0)
Stack: ffffffff882d6abd ffff81020e9d5300 ffff8102004f3470
0000000000000000
 0000000000000008 ffff810214841d78 0000000000000010 ffff810211beb000
 0000000000000010 ffff810000000000 ffffffff882d059f 0000000000000000
Call Trace:
 [<ffffffff882d6abd>] :vzcpt:dump_one_inode+0x71c/0xf66
 [<ffffffff882d059f>] :vzcpt:file_write+0x49/0x80
 [<ffffffff882d78a7>] :vzcpt:cpt_dump_files+0x86/0x2b4
 [<ffffffff882ce61e>] :vzcpt:cpt_dump+0x264/0x5af
 [<ffffffff882cc99b>] :vzcpt:cpt_ioctl+0x4f1/0xb82

[<ffffffff882cc4aa>] :vzcpt:cpt_ioctl+0x0/0xb82
[<ffffffff802e1e47>] proc_reg_unlocked_ioctl+0xb2/0xd2
[<ffffffff802b4461>] do_ioctl+0x21/0x6b
[<ffffffff802b46f8>] vfs_ioctl+0x24d/0x266
[<ffffffff802a831d>] vfs_write+0x121/0x156
[<ffffffff802b474d>] sys_ioctl+0x3c/0x5f
[<ffffffff8020c03e>] system_call+0x7e/0x83

Code: Bad RIP value.
RIP [<0000000000000000>] _stext+0x7fdf7000/0x1a
RSP <ffff810214841d00>
CR2: 0000000000000000
---[end trace a0f5c78b04d02c56]---
proxmox-104:~#

Subject: Re: 2.6.24 bug report: problems with vzmigrate
Posted by Alexey Dobriyan on Wed, 19 Mar 2008 12:41:35 GMT
View Forum Message <> Reply to Message

On Mon, Mar 17, 2008 at 12:29:44PM +0100, Dietmar Maurer wrote:
> [<ffffffff882d6abd>] :vzcpt:dump_one_inode+0x71c/0xf66
> [<ffffffff882d059f>] :vzcpt:file_write+0x49/0x80
> [<ffffffff882d78a7>] :vzcpt:cpt_dump_files+0x86/0x2b4
> [<ffffffff882ce61e>] :vzcpt:cpt_dump+0x264/0x5af
> [<ffffffff882cc99b>] :vzcpt:cpt_ioctl+0x4f1/0xb82
> [<ffffffff882cc4aa>] :vzcpt:cpt_ioctl+0x0/0xb82
> [<ffffffff802e1e47>] proc_reg_unlocked_ioctl+0xb2/0xd2
> [<ffffffff802b4461>] do_ioctl+0x21/0x6b
> [<ffffffff802b46f8>] vfs_ioctl+0x24d/0x266
> [<ffffffff802a831d>] vfs_write+0x121/0x156
> [<ffffffff802b474d>] sys_ioctl+0x3c/0x5f
> [<ffffffff8020c03e>] system_call+0x7e/0x83

Thanks, for report. It lives as
http://bugzilla.openvz.org/show_bug.cgi?id=850
from now.
