Subject: [PATCH] skip data conversion in compat_sys_mount when data_page is NULL
Posted by Andrey Mirkin on Fri, 01 Dec 2006 11:21:56 GMT
View Forum Message <> Reply to Message

OpenVZ Linux kernel team has found a problem with mounting in compat mode.

Simple command "mount -t smbfs ..." on Fedora Core 5 distro in 32-bit mode
leads to oops:

Unable to handle kernel NULL pointer dereference at 0000000000000000 RIP:
[<ffffffff802bc7c6>] compat_sys_mount+0xd6/0x290
PGD 34d48067 PUD 34d03067 PMD 0
Oops: 0000 [1] SMP
CPU: 0
Modules linked in: iptable_nat simfs smbfs ip_nat ip_conntrack vzdquota
parport_pc lp parport 8021q bridge llc vznetdev vzmon nfs lockd sunrpc vzdev
iptable_filter af_packet xt_length ipt_ttl xt_tcpmss ipt_TCPMSS
iptable_mangle xt_limit ipt_tos ipt_REJECT ip_tables x_tables thermal
processor fan button battery asus_acpi ac uhci_hcd ehci_hcd usbcore i2c_i801
i2c_core e100 mii floppy ide_cd cdrom
Pid: 14656, comm: mount
RIP: 0060:[<ffffffff802bc7c6>] [<ffffffff802bc7c6>]
compat_sys_mount+0xd6/0x290
RSP: 0000:ffff810034d31f38 EFLAGS: 00010292
RAX: 000000000000002c RBX: 0000000000000000 RCX: 0000000000000000
RDX: ffff810034c86bc0 RSI: 0000000000000096 RDI: ffffffff8061fc90
RBP: ffff810034d31f78 R08: 0000000000000000 R09: 000000000000000d
R10: ffff810034d31e58 R11: 0000000000000001 R12: ffff810039dc3000
R13: 000000000805ea48 R14: 0000000000000000 R15: 00000000c0ed0000
FS: 0000000000000000(0000) GS:ffffffff80749000(0033) knlGS:00000000b7d556b0
CS: 0060 DS: 007b ES: 007b CR0: 000000008005003b
CR2: 0000000000000000 CR3: 0000000034d43000 CR4: 00000000000006e0
Process mount (pid: 14656, veid=300, threadinfo ffff810034d30000, task
ffff810034c86bc0)
Stack: 0000000000000000 ffff810034dd0000 ffff810034e4a000 000000000805ea48
0000000000000000 0000000000000000 0000000000000000 0000000000000000
000000000805ea48 ffffffff8021e64e 0000000000000000 0000000000000000
Call Trace:
[<ffffffff8021e64e>] ia32_sysret+0x0/0xa

Code: 83 3b 06 0f 85 41 01 00 00 0f b7 43 0c 89 43 14 0f b7 43 0a
RIP [<ffffffff802bc7c6>] compat_sys_mount+0xd6/0x290
RSP <ffff810034d31f38>
CR2: 0000000000000000

The problem is that data_page pointer can be NULL, so we should skip data

conversion in this case.

Signed-Off-By: Andrey Mirkin <amirkin@openvz.org>

--

```
diff --git a/fs/compat.c b/fs/compat.c
index 8d0a001..7c8dd28 100644
--- a/fs/compat.c
+++ b/fs/compat.c
@@ -869,7 +869,7 @@ asmlinkage long compat_sys_mount(char __

  retval = -EINVAL;

- if (type_page) {
+ if (type_page && data_page) {
   if (!strcmp((char *)type_page, SMBFS_NAME)) {
    do_smb_super_data_conv((void *)data_page);
   } else if (!strcmp((char *)type_page, NCPFS_NAME)) {
```