
Subject: Re: syslog "kernel: BUG: unable to handle kernel NULL pointer dereference"

Posted by [Vasily Tarasov](#) on Tue, 27 Jan 2004 21:04:51 GMT

[View Forum Message](#) <> [Reply to Message](#)

Hello, since 028test10 kernel a number of fixes were introduced in iptables. Particularly, this patch is very pertinent:

<http://git.openvz.org/?p=linux-2.6.18-openvz;a=commit;h=376c9a91a99f709082f60f701fd74f0887f2b97b>

So, please, upgrade till recent kernel and inform us if the Ooops will survive.

Thanks,
Vasily.

Stuart MacIntosh wrote:

```
> My OVZ server printed an EIP late last night when I ran my ip6tables
> script. I'm no kernel hacker but thought someone on this list may want
> to know.
> My ip6tables command on both the HN and VE stopped working at the same
> time. for example 'ip6tables -P INPUT DROP' just hangs but iptables
> (IPv4) still works. Havn't rebooted yet in case I can help debug something.
>
> baikonour:/etc/init.d# uname -a
> Linux baikonour 2.6.18-028test010.1-ovz-smp #1 SMP Fri Jan 12 22:20:35
> CET 2007 i686 GNU/Linux
> baikonour:~# ip6tables -V
> ip6tables v1.3.6
> baikonour:~# cat /proc/version
> Linux version 2.6.18-028test010.1-ovz-smp (root@build32.sarge.sysys.org)
> (gcc version 3.3.5 (Debian 1:3.3.5-13)) #1 SMP Fri Jan 12 22:20:35 CET 2007
> baikonour:~# vzctl --version
> vzctl version 3.0.14-1dso31.2
>
>
> --- syslog messages follow ---
> Mar 11 02:49:58 baikonour kernel: BUG: unable to handle kernel NULL
> pointer dereference at virtual address 00000000
> Mar 11 02:49:58 baikonour kernel: printing eip:
> Mar 11 02:49:58 baikonour kernel: e0b2abe3
> Mar 11 02:49:58 baikonour kernel: *pde = 00000000
> Mar 11 02:49:58 baikonour kernel: Oops: 0000 [#1]
> Mar 11 02:49:58 baikonour kernel: SMP
> Mar 11 02:49:58 baikonour kernel: Modules linked in: ip6t_LOG
> ip6table_filter ip6_tables bridge llc xt_mac ipt_LOG xt_state
> iptable_nat nfs lockd sunrpc simfs vznetdev vzethdev vzrst ip_nat vzcpt
> ip_conntrack vxdquota vzmon vzdev xt_tcpudp xt_length ipt_ttl xt_tcpmss
```

```

> ipt_TCPMSS iptable_mangle iptable_filter xt_multiport xt_limit ipt_tos
> ipt_REJECT ip_tables x_tables af_packet i2c_piix4 i2c_core shpchp
> uhci_hcd usbcore 3c59x mii ide_cd cdrom
> Mar 11 02:49:58 baikonour kernel: CPU: 1, VCPU: 101.0
> Mar 11 02:49:58 baikonour kernel: EIP: 0060:[<e0b2abe3>] Not
> tainted VLI
> Mar 11 02:49:58 baikonour kernel: EFLAGS: 00010286
> (2.6.18-028test010.1-ovz-smp #1)
> Mar 11 02:49:58 baikonour kernel: EIP is at xt_find_table_lock+0x43/0xe0
> [x_tables]
> Mar 11 02:49:58 baikonour kernel: eax: c5fae800 ebx: 0000000a ecx:
> 00000000 edx: dca9b000
> Mar 11 02:49:58 baikonour kernel: esi: 00000050 edi: 00000040 ebp:
> bf940260 esp: cbb91dac
> Mar 11 02:49:58 baikonour kernel: ds: 007b es: 007b ss: 0068
> Mar 11 02:49:58 baikonour kernel: Process ip6tables (pid: 31695, veid:
> 101, ti=cbb90000 task=c5fae800 task.ti=cbb90000)
> Mar 11 02:49:58 baikonour kernel: Stack: bf940260 cbb91f1c 00000040
> 00000040 bf940260 e0c21b85 0000000a cbb91e94
> Mar 11 02:49:58 baikonour kernel: 00000020 c0198c0d cbb91de4
> 00000000 dcc5ae44 b7f91000 b7f91000 c0164f02
> Mar 11 02:49:58 baikonour kernel: dcc5ae40 00000007 00000000
> c140bcb4 00000000 00000000 c9a1f600 b7f91000
> Mar 11 02:49:58 baikonour kernel: Call Trace:
> Mar 11 02:49:58 baikonour kernel: [<e0c21b85>]
> do_ip6t_get_ctl+0x135/0x310 [ip6_tables]
> Mar 11 02:49:58 baikonour kernel: [<c0198c0d>] touch_atime+0x7d/0xe0
> Mar 11 02:49:58 baikonour kernel: [<c0164f02>] zap_pte_range+0x102/0x300
> Mar 11 02:49:58 baikonour kernel: [<c02b3373>] prio_tree_remove+0x83/0x100
> Mar 11 02:49:58 baikonour kernel: [<c015b632>] prep_new_page+0x112/0x1d0
> Mar 11 02:49:58 baikonour kernel: [<c01414d8>]
> change_slab_charged+0x108/0x130
> Mar 11 02:49:58 baikonour kernel: [<c0492479>] nf_sockopt+0xc9/0x140
> Mar 11 02:49:58 baikonour kernel: [<c0492568>] nf_getsockopt+0x38/0x40
> Mar 11 02:49:58 baikonour kernel: [<c04eee18>] ipv6_getsockopt+0xe8/0x110
> Mar 11 02:49:58 baikonour kernel: [<c04724a3>]
> sock_common_getsockopt+0x33/0x40
> Mar 11 02:49:58 baikonour kernel: [<c046fa59>] sys_getsockopt+0x69/0xc0
> Mar 11 02:49:58 baikonour kernel: [<c0470159>] sys_socketcall+0x229/0x260
> Mar 11 02:49:58 baikonour kernel: [<c01158a0>] do_page_fault+0x0/0x510
> Mar 11 02:49:58 baikonour kernel: [<c010311f>] syscall_call+0x7/0xb
> Mar 11 02:49:58 baikonour kernel: Code: 89 f0 29 d8 8d 04 c2 e8 5c 08 9e
> df 85 c0 ba fc ff ff ff 75 69 89 e0 25 00 e0 ff ff 8b 00 8b
> 90 8c 05 00 00 8b 8c da f8 08 00 00 <8b> 01 8d 74 26 00 8d 94 16 f8 08
> 00 00 39 d1 74 6d 89 34 24 89
> Mar 11 02:49:58 baikonour kernel: EIP: [<e0b2abe3>]
> xt_find_table_lock+0x43/0xe0 [x_tables] SS:ESP 0068:cbb91dac
> --- end of relevant syslog entries ---

```

>
>
> If I can provide you with any more relevant information to help let me know.
> Or if I'm just retarded and broke it myself by setting the wrong limits
> (quite possible) sorry!
> -Stuart
>
>
