OpenVZ OVZ-7188

Crash kernel 3.10.0-1062.4.2.vz7.116.7

Details

Type:	Bug	Status:	VERIFIED
Priority:	Critical	Resolution:	Fixed
Component/s:	Containers::Kernel	Fix Version/s:	Vz7.0-Update14
		Security Level:	Public

Environment:
- OS: CentOS 7
- Kernel: 3.10.0-1062.4.2.vz7.116.7
- vzctl version: 7.0.209-1
- ploop version: 7.0.163-1

Description

NB! If you know how to reproduce the problem
Please add "slub_debug=FPZU" to kernel commandline
however be ready that it will affect node performance.
see https://www.kernel.org/doc/Documentation/vm/slub.txt for details.

Denis Maksimov (elky):
Hello!

We have node crash on '3.10.0-1062.4.2.vz7.116.7' with:

```
[336695.185550] general protection fault: 0000 [#1] SMP
[336695.186061] Modules linked in: nf_conntrack_tftp nf_conntrack_snmp nf_conntrack_sane nf_conntrack_pptp nf_conntrack_proto_gre nf_conntrack_netbios_ns nf_conntrack_broadcast nf_conntrack_irc
nf_conntrack_h323 ts_kmp nf_conntrack_amanda xt_CT sch_sfq cls_u32 ip_set xt_TCPMSS nft_meta nft_compat nft_counter nf_tables_ipv4 ip6t_REJECT nf_reject_ipv6 xt_nat nf_log_ipv4 nf_log_common xt_limit ipt_REJECT
nf_reject_ipv4 xt_conntrack xt_multiport xt_addrtype nf_conntrack_sip nf_conntrack_netlink binfmt_misc nf_tables nfnetlink ip6table_mangle xt_mark raw_diag udp_diag tcp_diag inet_diag netlink_diag af_packet_diag
unix_diag nfsv3 nfs_acl rpcsec_gss_krb5 auth_rpcgss nfsv4 dns_resolver 8021q garp mrp bonding ip6table_filter ip6_tables xt_comment iptable_filter iTCO_wdt iTCO_vendor_support dcdbas sb_edac ipip
[336695.193828] tunnel4 ipmi_ssif ip_tunnel intel_powerclamp i2c_algo_bit ttm coretemp nfs intel_rapl drm_kms_helper iosf_mbi syscopyarea kvm_intel sysfillrect sysimgblt lockd fb_sys_fops grace kvm drm sunrpc joydev
mei_me irqbypass fscache drm_panel_orientation_quirks mei ipmi_si wmi ipmi_devintf sg acpi_pad ipmi_msghandler acpi_power_meter nf_conntrack_ftp lpc_ich xt_recent pcc_cpufreq ipt_MASQUERADE
nf_nat_masquerade_ipv4 iptable_raw iptable_mangle xt_connlimit xt_REDIRECT nf_nat_redirect xt_owner nf_conntrack_ipv6 nf_defrag_ipv6 xt_state xt_LOG xfrm_ipcomp xfrm4_mode_transport xfrm6_mode_tunnel
xfrm4_mode_tunnel esp6 esp4 af_key ip_vs arc4 br_netfilter veth ppp_mppe overlay ppp_deflate ppp_async ppp_generic slhc ip6_vzprivnet crc_ccitt ip6_vznetstat fuse ip_vznetstat ip_vzprivnet vziolimit vzevent
[336695.202453] vzlist iptable_nat vzstat nf_conntrack_ipv4 vznetdev nf_defrag_ipv4 vzmon bridge nf_nat_ipv4 nf_nat stp llc nf_conntrack libcrc32c pio_kaio tun pio_nfs pio_direct pfmt_raw pfmt_ploop1 vznetstat ploop
vzdev nbd sch_htb ip_tables ext4 mbcache jbd2 sd_mod crc_t10dif crct10dif_generic crct10dif_pclmul crct10dif_common crc32_pclmul crc32c_intel ghash_clmulni_intel aesni_intel lrw gf128mul tg3 glue_helper ablk_helper
cryptd megaraid_sas ptp pps_core dm_mirror dm_region_hash dm_log dm_mod
[336695.208398] CPU: 26 PID: 0 Comm: swapper/26 ve: 0 Kdump: loaded Not tainted 3.10.0-1062.4.2.vz7.116.7 #1 116.7
[336695.208988] Hardware name: Dell Inc. PowerEdge R720xd/0W7JN5, BIOS 2.9.0 12/06/2019
[336695.209567] task: ffff968e76ebe000 ti: ffff968e76ec4000 task.ti: ffff968e76ec4000
[336695.210148] RIP: 0010:[<ffffffffa14f5126>] [<ffffffffa14f5126>] addr_same+0x6/0x50
[336695.210913] RSP: 0018:ffff96bcafb439e8 EFLAGS: 00010282
[336695.211250] RAX: 0000000000000000 RBX: b8e3884beafeceda RCX: 0000000000001274
[336695.211825] RDX: 000000000000579a RSI: ffff96bcafb43a30 RDI: b8e3884beafecee2
[336695.212405] RBP: ffff96bcafb43a18 R08: 00000000000016d0 R09: ffffffffa16a8ca0
[336695.212988] R10: 0000000043e73db1 R11: 0000000000000000 R12: 0000000000000002
[336695.213575] R13: ffff96bcafb43a30 R14: ffff96bcafb43a50 R15: ffff96bcafb43a50
[336695.214161] FS: 0000000000000000(0000) GS:ffff96bcafb40000(0000) knlGS:0000000000000000
[336695.214752] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[336695.215096] CR2: 00007f9c678c5000 CR3: 00000035bc410000 CR4: 00000000001607e0
[336695.215687] Call Trace:
[336695.216027] <IRQ>
[336695.216125] [<ffffffffa14f51ac>] ? __tcp_get_metrics.isra.7+0x3c/0x80
[336695.216797] [<ffffffffa14f600f>] tcp_get_metrics+0xbf/0x2e0
[336695.217135] [<ffffffffa1520002>] ? ipmr_mfc_add+0x2a2/0x5e0
[336695.217474] [<ffffffffa1460002>] ? compat_sock_ioctl+0x6e2/0x950
[336695.217810] [<ffffffffa14f64a9>] tcp_init_metrics+0x49/0x1c0
[336695.218151] [<ffffffffa1523f4c>] ? bictcp_init+0xac/0xf0
[336695.218496] [<ffffffffa14e7832>] tcp_rcv_state_process+0xcb2/0xf50
[336695.218836] [<ffffffffa14f3b52>] ? tcp_check_req+0x462/0x5b0
[336695.219176] [<ffffffffa14f3d05>] tcp_child_process+0x65/0x170
[336695.219516] [<ffffffffa14f1545>] tcp_v4_do_rcv+0x265/0x350
[336695.219859] [<ffffffffa14f2bed>] tcp_v4_rcv+0x7dd/0x9e0
[336695.220197] [<ffffffffa14cacc5>] ip_local_deliver_finish+0xe5/0x220
[336695.220548] [<ffffffffa14cafb0>] ip_local_deliver+0x60/0xe0
[336695.220892] [<ffffffffa14cabe0>] ? ip_rcv_finish+0x370/0x370
[336695.221233] [<ffffffffa14ca900>] ip_rcv_finish+0x90/0x370
[336695.221568] [<ffffffffa14cb2f0>] ip_rcv+0x2c0/0x420
[336695.221906] [<ffffffffa14ca870>] ? inet_del_offload+0x40/0x40
[336695.222242] [<ffffffffa147f439>] __netif_receive_skb_core+0x729/0xa10
[336695.222580] [<ffffffffa147f738>] __netif_receive_skb+0x18/0x60
[336695.222926] [<ffffffffa148070e>] process_backlog+0xae/0x180
[336695.223273] [<ffffffffa147fdef>] net_rx_action+0x27f/0x3a0
[336695.223616] [<ffffffffa15c5125>] __do_softirq+0x125/0x2bb
[336695.223956] [<ffffffffa15c158c>] call_softirq+0x1c/0x30
[336695.224300] [<ffffffffa0e2f645>] do_softirq+0x65/0xa0
[336695.224643] [<ffffffffa0ea5d55>] irq_exit+0x105/0x110
[336695.225077] [<ffffffffa15c4986>] do_IRQ+0x56/0xf0
[336695.225421] [<ffffffffa15b636a>] common_interrupt+0x16a/0x16a
[336695.225756] <EOI>
[336695.225845] [<ffffffffa13f0837>] ? cpuidle_enter_state+0x57/0xd0
[336695.226510] [<ffffffffa13f098e>] cpuidle_idle_call+0xde/0x230
[336695.226854] [<ffffffffa0e3833e>] arch_cpu_idle+0xe/0xc0
[336695.227191] [<ffffffffa0f06b6a>] cpu_startup_entry+0x14a/0x1e0
[336695.227529] [<ffffffffa0e5ab47>] start_secondary+0x1f7/0x270
[336695.227879] [<ffffffffa0e000d5>] start_cpu+0x5/0x14
[336695.228217] Code: 02 00 00 48 d3 e7 e8 ca b3 af ff 48 83 f8 01 48 89 83 88 02 00 00 19 c0 5b 83 e0 f4 5d c3 0f 1f 80 00 00 00 00 0f 1f 44 00 00 55 <0f> b7 57 10 31 c0 66 3b 56 10 48 89 e5 74 0b 5d c3 66 0f 1f 84
```

```
[336695.234230] RIP [<ffffffffa14f5126>] addr_same+0x6/0x50
[336695.234649] RSP <ffff96bcafb439e8>
```

We can upload core dumps if it need and etc.

Activity

19 older comments

Vasily Averin added a comment - 08/Jun/20 10:34 AM

there is difference vs crash 27.04
27.04 – nf conn_nat was present, corrupted 2 bytes with offset 0xa and 0xb beyond end of object
now – nf_conn_help was presnst, corrupt 2 bytes with offset 0x2 and 0x3 beyond end of object

Vasily Averin added a comment - 08/Jun/20 12:30 PM

struct nf_conntrack_helper __rcu *helper; == 0xffffffffc08aaa60
it points to second element of nf_conntrack_helper_q931 array,
I've noticed that it lacks for .data_len definition, need to check is it important or not

Vasily Averin added a comment - 09/Jun/20 10:42 AM

sent to devel@openvz.org
[patch RH7] netfilter: nf_conntrack_h323: lost .data_len definition for Q.931/ipv6

Jira Sync added a comment - 09/Jun/20 11:45 AM

The commit is pushed to "branch-rh7-3.10.0-1127.8.2.vz7.151.x-ovz" and will appear at https://src.openvz.org/scm/ovz/vzkernel.git
after rh7-3.10.0-1127.8.2.vz7.151.13
------>
commit 5b730c71a3ad454effdc33f4ef373e1abfd56f73
Author: Vasily Averin <vvs@virtuozzo.com>
Date: Tue Jun 9 12:34:24 2020 +0300

netfilter: nf_conntrack_h323: lost .data_len definition for Q.931/ipv6

Jira Sync added a comment - 09/Jun/20 9:35 PM

Fixed.

People

Assignee:

Vasily Averin

Reporter:

Denis Maksimov

Votes:

1 Vote for this issue

Watchers:

4 Start watching this issue

Dates

Created:

27/Feb/20 11:20 PM

Updated:

09/Jun/20 9:35 PM

Resolved:

09/Jun/20 11:45 AM