Subject: Re: [PATCH 00/17] Pid-NS(V3) Enable multiple pid namespaces
Posted by Alexey Dobriyan on Fri, 22 Jun 2007 12:53:23 GMT
View Forum Message <> Reply to Message

It crashed while playing with your version of pid namespaces.

We created namespace, entered it, run perf.c benchmark
and mount /proc; umount /proc loop.

BUG: unable to handle kernel NULL pointer dereference at virtual address 0000004c
printing eip:
*pde = 00000000
Oops: 0000 [#1]
SMP
Modules linked in: sbs button battery ac sky2 e1000 ata_piix libata sd_mod scsi_mod
CPU: 1
EIP: 0060:[<c0465fb2>] Not tainted VLI
EFLAGS: 00010246 (2.6.22-rc4-mm2-pidns-y #2)
EIP is at d_hash_and_lookup+0x36/0x63
eax: 00135738 ebx: c52bff30 ecx: ffffffff edx: 00000003
esi: c52bff1c edi: 00d4bf68 ebp: 00000000 esp: c52bfef0
ds: 007b es: 007b fs: 00d8 gs: 0000 ss: 0068
Process perf (pid: 29058, ti=c52be000 task=c52b4370 task.ti=c52be000)
Stack: 00000000 c40dc0c0 c52b4370 00000000 c52bff2c c0480225 c52bff2c 0000000d
c05d7a23 000019af 00000001 00d4bf68 00000004 c52bff2c 00000000 35373536
00000000 00000000 3a221caa c4716e80 c4716eb0 00000001 c52b4370 c048032f
Call Trace:
[<c0480225>] proc_flush_task_from_pid_ns+0xf5/0x1d7
[<c048032f>] proc_flush_task+0x28/0x2f
[<c041ce15>] release_task+0xc/0xcb
[<c041dc1a>] exit_notify+0x229/0x230
[<c041df5d>] do_exit+0x33c/0x392
[<c041dfd3>] do_group_exit+0x0/0x6d
[<c0402500>] syscall_call+0x7/0xb
=======================
Code: c7 04 24 00 00 00 00 8b 5a 08 8b 4a 04 49 83 f9 ff 74 16 0f b6 13 43 89 d0 c1 e0 04 8d 04 07 c1 ea 04 01 d0 6b f8 0b eb e4 89 3e <8b> 45 4c 85 c0 74 11 8b 48 04 85 c9 74 0a 89 f2 89 e8 ff d1 85
EIP: [<c0465fb2>] d_hash_and_lookup+0x36/0x63 SS:ESP 0068:c52bfef0

_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers