

# panic in tcp\_discardcb()

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2006-11/msg00248.html>

---

- *From:* Pav Lucistnik <[pav@xxxxxxxxxxxx](mailto:pav@xxxxxxxxxxxx)>
  - *Date:* Tue, 28 Nov 2006 14:27:10 +0100
- 

Hey,

Can anyone make anything out of this panic? It's SMP 6.1-RELEASE on i386. (Yes I know 6.1 is oold, but it's the latest available release currently, so, it's what we have in production.)

kernel trap 12 with interrupts disabled

```
Fatal trap 12: page fault while in kernel mode
cpuid = 0; apic id = 00
fault virtual address = 0x0
fault code = supervisor write, page not present
instruction pointer = 0x20:0xc056b627
stack pointer = 0x28:0xd440ab24
frame pointer = 0x28:0xd440ab30
code segment = base 0x0, limit 0xffff, type 0x1b
= DPL 0, pres 1, def32 1, gran 1
processor eflags = resume, IOPL = 0
current process = 13 (swi1: net)
trap number = 12
panic: page fault
cpuid = 0
Uptime: 73d21h24m3s
```

(kgdb) bt

```
#0 doadump () at pcpu.h:165
#1 0xc055e50d in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:402
#2 0xc055e835 in panic (fmt=0xc0706511 "%s") at /usr/src/sys/kern/kern_shutdown.c:558
#3 0xc06dee30 in trap_fatal (frame=0xd440aae4, eva=0) at /usr/src/sys/i386/i386/trap.c:836
#4 0xc06de5e6 in trap (frame=
{tf_fs = -1067909112, tf_es = -996671448, tf_ds = -734003160, tf_edi = 0, tf_esi = -998460540, tf_ebp =
-733959376, tf_esp = -733959408, tf_ebx = -1020302720, tf_edx = 0, tf_ecx = 0, tf_eax = 0, tf_trapno = 12,
tf_err = 2, tf_eip = -1068059097, tf_cs = 32, tf_eflags = 65538, tf_esp = 0, tf_ss = -998460976}) at
/usr/src/sys/i386/i386/trap.c:269
#5 0xc06cc0ca in calltrap () at /usr/src/sys/i386/i386/exception.s:139
#6 0xc056b627 in _callout_stop_safe (c=0xc47cb384, safe=0) at /usr/src/sys/kern/kern_timeout.c:553
#7 0xc05f3723 in tcp_discardcb (tp=0xc47cb1d0) at /usr/src/sys/netinet/tcp_subr.c:689
#8 0xc05f4e9d in tcp_twstart (tp=0xc47cb1d0) at /usr/src/sys/netinet/tcp_subr.c:1708
```

## panic in tcp\_discardcb()

```
#9 0xc05f0724 in tcp_input (m=0xc4e3e600, off0=20) at /usr/src/sys/netinet/tcp_input.c:2432
#10 0xc05e770d in ip_input (m=0xc4e3e600) at /usr/src/sys/netinet/ip_input.c:786
#11 0xc05d6717 in netisr_processqueue (ni=0xc07842f8) at /usr/src/sys/net/netisr.c:236
#12 0xc05d6916 in swi_net (dummy=0x0) at /usr/src/sys/net/netisr.c:349
#13 0xc05492d5 in ithread_execute_handlers (p=0xc32f5624, ie=0xc3337b80) at
/usr/src/sys/kern/kern_intr.c:684
#14 0xc05493f1 in ithread_loop (arg=0xc32bb8a0) at /usr/src/sys/kern/kern_intr.c:767
#15 0xc0548071 in fork_exit (callout=0xc054939c <ithread_loop>, arg=0xc32bb8a0, frame=0xd440ad38) at
/usr/src/sys/kern/kern_fork.c:805
#16 0xc06cc12c in fork_trampoline () at /usr/src/sys/i386/i386/exception.s:208
(kgdb) up 7
#7 0xc05f3723 in tcp_discardcb (tp=0xc47cb1d0) at /usr/src/sys/netinet/tcp_subr.c:689
689 callout_stop(tp->tt_delack);
(kgdb) print *tp
$2 = {t_segq = {lh_first = 0x0}, t_segqlen = 0, t_dupacks = 0, tt_rexmt = 0xc47cb314, tt_persist =
0xc47cb330, tt_keep = 0xc47cb34c, tt_2msl = 0xc47cb368, tt_delack = 0xc47cb384, t_inpcb = 0xc53e59d8,
t_state = 9, t_flags = 533, snd_una = 1473244779, snd_max = 1473244779, snd_nxt = 1473244779, snd_up =
1473239551, snd_wll = 2071426398, snd_wl2 = 1473244779, iss = 1473217650, irs = 2071426082,
rcv_nxt = 2071426399, rcv_adv = 2071491933, rcv_wnd = 65700, rcv_up = 2071426398, snd_wnd = 16673,
snd_cwnd = 6428, snd_bwnd = 3311178, snd_ssthresh = 2920, snd_bandwidth = 1517898, snd_recover =
1473244779,
t_maxopd = 1460, t_rcvtime = 2089746807, t_starttime = 2089699567, t_rtttime = 0, t_rtseq = 1473239551,
t_bw_rtttime = 2089746807, t_bw_rtseq = 1473244779, t_rxtcur = 4300, t_maxseg = 1460, t_srtt = 65645,
t_rttvar = 8198, t_rxtshift = 0, t_rttmin = 3, t_rttbest = 73843, t_rttupdated = 4, max_sndwnd = 17520,
t_softerror = 0, t_oobflags = 0 '\0', t_iobc = 0 '\0', snd_scale = 0 '\0', rcv_scale = 0 '\0',
request_r_scale = 0 '\0', requested_s_scale = 0 '\0', ts_recent = 0, ts_recent_age = 0, last_ack_sent =
2071426398, snd_cwnd_prev = 5840, snd_ssthresh_prev = 1073725440, snd_recover_prev = 1473217651,
t_badrxtwin = 2089702850, snd_limited = 2 '\002', rcv_second = 0, rcv_pps = 0, rcv_byps = 0, sack_enable =
1, snd_numholes = 0, snd_holes = {tqh_first = 0x0, tqh_last = 0xc47cb2c4}, snd_fack = 1473230791,
rcv_numsacks = 0, sackblks = {{start = 0, end = 0}, {start = 0, end = 0}, {start = 0, end = 0}, {start = 0, end =
0}, {start = 0, end = 0}, {start = 0, end = 0}}, sack_newdata = 1473230791, sackhint = {
nexthole = 0x0, sack_bytes_rexmit = 0}, t_rttlow = 1827}
(kgdb) print *tp->tt_delack
$4 = {c_links = {sle = {sle_next = 0x0}, tqe = {tqe_next = 0x0, tqe_prev = 0x0}}, c_time = -998460220,
c_arg = 0xc47cb4e0, c_func = 0xc47cb4fc, c_mtx = 0xc47cb518, c_flags = -998460112}
(kgdb) print *tp->tt_keep
$5 = {c_links = {sle = {sle_next = 0x0}, tqe = {tqe_next = 0x0, tqe_prev = 0xcd7511c8}}, c_time =
2096946807, c_arg = 0xc47cb1d0, c_func = 0xc05f7650 <tcp_timer_keep>, c_mtx = 0x0, c_flags = 16}
(kgdb) print *tp->tt_2msl
$6 = {c_links = {sle = {sle_next = 0x0}, tqe = {tqe_next = 0x0, tqe_prev = 0xcd7567c8}}, c_time =
2090346807, c_arg = 0xc47cb1d0, c_func = 0xc05f72f8 <tcp_timer_2msl>, c_mtx = 0x0, c_flags = 0}
(kgdb) print *tp->tt_persist
$7 = {c_links = {sle = {sle_next = 0x0}, tqe = {tqe_next = 0x0, tqe_prev = 0x0}}, c_time = 0, c_arg = 0x0,
c_func = 0, c_mtx = 0x0, c_flags = 16}
(kgdb) print *tp->tt_rexmt
$8 = {c_links = {sle = {sle_next = 0x0}, tqe = {tqe_next = 0x0, tqe_prev = 0xcd74af40}}, c_time =
2089751078, c_arg = 0xc47cb1d0, c_func = 0xc05f7b8c <tcp_timer_rexmt>, c_mtx = 0x0, c_flags = 16}
```

This looks to me as tt\_delack is corrupted somehow...?

panic in tcp\_discardcb()

--

Pav Lucistnik <pav@xxxxxxx>  
<pav@xxxxxxxxxxxx>

I want to earn the right to be obnoxious before I'm too bitter to really  
enjoy it.

-- Able

***Attachment: signature.asc***

*Description:* Toto je =?UTF-8?Q?digit=C3=A1ln=C4=9B?= =?ISO-8859-1?Q?\_podepsan=E1?=  
=?UTF-8?Q?\_=C4=8D=C3=A1st?= =?ISO-8859-1?Q?\_zpr=E1vy?=-