

Panic in _mtx_lock_sleep

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2003-11/0095.html>

From: Eivind Olsen (*eivind_at_aminor.no*)

Date: 11/02/03

Date: Sun, 02 Nov 2003 22:19:19 +0100
To: freebsd-current@freebsd.org

Hello. I just had a panic here. I'm running CURRENT as of 31st of October, platform is i386. I have a crashdump available if anyone wants to take a look at this.

Here's some output from gdb -k:

```
eivind@vimes:~/tmp/debug/2003-10-31 > gdb -k kernel.debug vmcore.6
GNU gdb 5.2.1 (FreeBSD)
Copyright 2002 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i386-undermydesk-freebsd"...
panic: from debugger
panic messages:
```

```
---
Fatal trap 12: page fault while in kernel mode
fault virtual address   = 0x68
fault code              = supervisor read, page not present
instruction pointer     = 0x8:0xc0647282
stack pointer          = 0x10:0xcfe919e0
frame pointer          = 0x10:0xcfe91a0c
code segment           = base 0x0, limit 0xfffff, type 0x1b
                       = DPL 0, pres 1, def32 1, gran 1
processor eflags       = interrupt enabled, resume, IOPL = 0
current process        = 326 (named)
panic: from debugger
Fatal trap 3: breakpoint instruction fault while in kernel mode
instruction pointer     = 0x8:0xc07f5914
stack pointer          = 0x10:0xcfe91794
frame pointer          = 0x10:0xcfe917a0
code segment           = base 0x0, limit 0xfffff, type 0x1b
                       = DPL 0, pres 1, def32 1, gran 1
processor eflags       = IOPL = 0
current process        = 326 (named)
panic: from debugger
Uptime: 19h17m7s
Fatal trap 12: page fault while in kernel mode
fault virtual address   = 0x24
```

freebsd-current: Panic in _mtx_lock_sleep

```
fault code          = supervisor read, page not present
instruction pointer  = 0x8:0xc0646edb
stack pointer       = 0x10:0xcb608aec
frame pointer       = 0x10:0xcb608b00
code segment        = base 0x0, limit 0xfffff, type 0x1b
                   = DPL 0, pres 1, def32 1, gran 1
processor eflags    = interrupt enabled, resume, IOPL = 0
current process     = 14 (swil: net)
panic: from debugger
Uptime: 19h17m8s
Dumping 191 MB
 16 32 48 64 80 96 112 128 144 160 176
---
```

Reading symbols from /boot/kernel/vinum.ko...done.

Loaded symbols from /boot/kernel/vinum.ko

#0 doadump () at /usr/src/sys/kern/kern_shutdown.c:240

240 dumping++;

(kgdb) bt

#0 doadump () at /usr/src/sys/kern/kern_shutdown.c:240

#1 0xc0651c90 in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:372

#2 0xc0652078 in panic () at /usr/src/sys/kern/kern_shutdown.c:550

#3 0xc0476f52 in db_panic () at /usr/src/sys/ddb/db_command.c:450

#4 0xc0476eb2 in db_command (last_cmdp=0xc09050e0, cmd_table=0x0, aux_cmd_tablep=0xc0889714, aux_cmd_tablep_end=0xc088972c) at /usr/src/sys/ddb/db_command.c:346

#5 0xc0476ff5 in db_command_loop () at /usr/src/sys/ddb/db_command.c:472

#6 0xc047a005 in db_trap (type=12, code=0) at /usr/src/sys/ddb/db_trap.c:73

#7 0xc07f565c in kdb_trap (type=12, code=0, regs=0xcfe919a0) at /usr/src/sys/i386/i386/db_interface.c:171

#8 0xc0807b76 in trap_fatal (frame=0xcfe919a0, eva=0) at /usr/src/sys/i386/i386/trap.c:818

#9 0xc0807183 in trap (frame=

```
    {tf_fs = -1033306088, tf_es = -1023934448, tf_ds = -806813680, tf_edi
= -1030808900, tf_esi = -1030785904, tf_ebp = -806807028, tf_esp =
-806807092, tf_ebx = -1033092512, tf_edx = 2, tf_ecx = 0, tf_eax = 1,
tf_trapno = 12, tf_err = 0, tf_eip = -1067158910, tf_cs = 8, tf_eflags =
66118, tf_esp = 42062, tf_ss = -806807052}) at
/usr/src/sys/i386/i386/trap.c:252
```

#10 0xc07f7008 in calltrap () at {standard input}:102

#11 0xc06ebab6 in ip_output (m0=0xc26c4260, opt=0xc28f7490, ro=0xc28f1abc, flags=0, imo=0x0, inp=0xc28f1a80) at /usr/src/sys/netinet/ip_output.c:266

#12 0xc06fd2d6 in udp_output (inp=0xc28f1a80, m=0xc1561300, addr=0xc2745660, control=0x0, td=0xc26c4260) at /usr/src/sys/netinet/udp_usrreq.c:847

#13 0xc06fdf81 in udp_send (so=0x0, flags=0, m=0xc155cf00, addr=0x0, control=0x0, td=0x0) at /usr/src/sys/netinet/udp_usrreq.c:1043

#14 0xc06913fd in sosend (so=0xc2913220, addr=0xc2745660, uio=0xcfe91bf4, top=0xc155cf00, control=0x0, flags=0, td=0xc26c4260) at /usr/src/sys/kern/uipc_socket.c:715

#15 0xc0695cdc in kern_sendit (td=0xc26c4260, s=22, mp=0xcfe91ca4, flags=0, control=0x0) at /usr/src/sys/kern/uipc_syscalls.c:722

#16 0xc0695afe in sendit (td=0x0, s=0, mp=0xcfe91ca4, flags=0) at /usr/src/sys/kern/uipc_syscalls.c:662

#17 0xc06960f3 in sendmsg (td=0x0, uap=0xcfe91d10) at /usr/src/sys/kern/uipc_syscalls.c:900

#18 0xc0807f30 in syscall (frame=

```
    {tf_fs = 135790639, tf_es = 135856175, tf_ds = -1078001617, tf_edi =
0, tf_esi = 0, tf_ebp = -1077943560, tf_esp = -806806156, tf_ebx = 0,
tf_edx = 135876352, tf_ecx = 136334080, tf_eax = 28, tf_trapno = 0, tf_err
= 2, tf_eip = 674256815, tf_cs = 31, tf_eflags = 646, tf_esp = -1077943988,
tf_ss = 47}) at /usr/src/sys/i386/i386/trap.c:1012
```

#19 0xc07f705d in Xint0x80_syscall () at {standard input}:144

freebsd-current: Panic in _mtx_lock_sleep

---Can't read userspace from dump, or kernel process---
(kgdb)

This is what I got from the kernel debugger:

Fatal trap 12: page fault while in kernel mode

fault virtual address = 0x68
fault code = supervisor read, page not present
instruction pointer = 0x8:0xc0647282
stack pointer = 0x10:0xcfe919e0
frame pointer = 0x10:0xcfe91a0c
code segment = base 0x0, limit 0xfffff, type 0x1b
= DPL 0, pres 1, def32 1, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = 326 (named)

kernel: type 12 trap, code=0

Stopped at _mtx_lock_sleep+0x1b2: movl 0x68(%ecx),%edx

db> show reg

```
cs          0x8
ds          0xcfe90010
es          0xc2f80010
fs          0xc2690018
ss          0x10
eax         0x1
ecx         0
edx         0x2
ebx         0xc26c4260
esp         0xcfe919e0
ebp         0xcfe91a0c
esi         0xc28f7490
edi         0xc28f1abc
eip         0xc0647282  _mtx_lock_sleep+0x1b2
efl         0x10246
dr0         0
dr1         0
dr2         0
dr3         0
dr4         0xffff0ff0
dr5         0x400
dr6         0xffff0ff0
dr7         0x400
_mtx_lock_sleep+0x1b2:  movl 0x68(%ecx),%edx
```

db> trace

```
_mtx_lock_sleep(c28f7490,0,0,0,0) at _mtx_lock_sleep+0x1b2
ip_output(c1561300,0,c28f1abc,0,0) at ip_input+0x296
udp_output(c28f1a80,c1561300,c2745660,0,c26c4260) at udp_output+0x406
udp_send(c2913220,0,c155cf00,c2745660,0) at udp_send+0x121
sosend(c2913220,c2745660,cfe91bf4,c155cf00,0) at sosend+0x43d
kern_sendit(c26c4260,16,cfe91ca4,0,0) at kern_sendit+0x1ac
sendit(c26c4260,16,cfe91ca4,0,bfbfe572) at sendit+0x16e
sendmsg(c26c4260,cfe91d10,c,c0679a26,3) at sendmsg+0xc3
syscall(818002f,819002f,bfbf002f,0,0) at syscall+0x310
Xint0x80_syscall() at Xint0x80_syscall+0x1d
-- syscall (28, FreeBSD ELF32, sendmsg), eip = 0x283057af, esp =
0xbfbfe14c, ebp = 0xbfbfe2f8 ---
```

db>

I then had to write "panic" two or three times until it started to do the crashdump.

--

Regards / Hilsen
Eivind Olsen
<eivind@aminor.no>

freebsd-current@freebsd.org mailing list

freebsd-current: Panic in _mtx_lock_sleep

<http://lists.freebsd.org/mailman/listinfo/freebsd-current>

To unsubscribe, send any mail to "freebsd-current-unsubscribe@freebsd.org"