

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2006-04/msg00432.html>

- *From:* Scott Long <scottl@xxxxxxxxxxx>
 - *Date:* Tue, 25 Apr 2006 23:47:35 -0600
-

I don't see how thread could have jumped from kern_sendit() to xpt_action(). There either are a whole lot of missing stack frames, or some freaky preemption happened that screwed up the stack.

Scott

Anish Mistry wrote:

On Wednesday 26 April 2006 00:55, Scott Long wrote:

This trace doesn't make much sense. Maybe FUSE is inappropriately messing with CAM internals?

Fuse doesn't seem to use CAM at all, and Fuse didn't have any active mounts anytime during that boot. I seriously doubt I can reproduce this so I guess it'll just be relegated to the archives. I do have a crash dump if anyone is interested.

Scott

Anish Mistry wrote:

I got the above panic from CURRENT as of April 19th. I wasn't running anything cam related, at least I don't think so. The system was just idle.

Unread portion of the kernel message buffer:
panic: mutex Giant not owned at
/usr/src/sys/cam/cam_xpt.c:4837
KDB: enter: panic
panic: from debugger

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

```
Uptime: 6h41m53s
Dumping 239 MB (2 chunks)
chunk 0: 1MB (156 pages) ... ok
chunk 1: 239MB (61152 pages) 223 207 191 175 159 143
127 111 95
79 63 47 31 15

#0 doadump () at pcpu.h:166
166 pcpu.h: No such file or directory.
in pcpu.h
(kgdb) bt
#0 doadump () at pcpu.h:166
#1 0xc04cc445 in boot (howto=260)
at /usr/src/sys/kern/kern_shutdown.c:409
#2 0xc04cbfa3 in panic (fmt=0xc061ce45 "from debugger")
at /usr/src/sys/kern/kern_shutdown.c:565
#3 0xc0442e2d in db_panic (addr=-1068598180,
have_addr=0,
count=-1, modif=0xcca4b958 "") at
/usr/src/sys/ddb/db_command.c:426 #4 0xc04431ba in
db_command_loop ()
at /usr/src/sys/ddb/db_command.c:395
#5 0xc0444da3 in db_trap (type=3, code=0)
at /usr/src/sys/ddb/db_main.c:221
#6 0xc04e807b in kdb_trap (type=3, code=0, tf=0x0)
at /usr/src/sys/kern/subr_kdb.c:481
#7 0xc05ff23c in trap (frame=
{tf_fs = 8, tf_es = 40, tf_ds = 40, tf_edi = -1030784912,
tf_esi = -1067285255, tf_ebp = -861619444, tf_isp =
-861619464,
tf_ebx = -861619404, tf_edx = -1067281663, tf_ecx =
-1056878592,
tf_eax = -1067272577, tf_trapno = 3, tf_err = 0, tf_eip =
-1068598180, tf_cs = 32, tf_eflags = 642, tf_esp =
-861619416,
tf_ss = -1068711934}) at /usr/src/sys/i386/i386/trap.c:622
#8 0xc05f0afa in calltrap ()
at /usr/src/sys/i386/i386/exception.s:138
#9 0xc04e7c5c in kdb_enter (msg=0xc062b67f "KDB: enter:
%s\n")
at cpufunc.h:60
#10 0xc04cc002 in panic (fmt=0xc06284f9 "mutex %s not
owned at
%s:%d") at /usr/src/sys/kern/kern_shutdown.c:549
#11 0xc04c3b43 in _mtx_assert (m=0xc06286ff,
what=-1056878592,
file=0xc06181c9 "/usr/src/sys/cam/cam_xpt.c", line=4837)
at /usr/src/sys/kern/kern_mutex.c:768
---Type <return> to continue, or q <return> to quit---
#12 0xc0432c65 in xpt_release_devq (path=0x0, count=1,
run_queue=1) at /usr/src/sys/cam/cam_xpt.c:4837
```

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

```
#13 0xc043420e in xpt_action (start_ccb=0xc22f9530)
at /usr/src/sys/cam/cam_xpt.c:3580
#14 0xc051091b in kern_sendit (td=0xc28f7870, s=4,
mp=0xccca4bc6c,
flags=0,
control=0x0, segflg=3227694719)
at /usr/src/sys/kern/uipc_syscalls.c:775
#15 0xc0511965 in sendit (td=0xc28f7870, s=4,
mp=0xccca4bc6c,
flags=0) at /usr/src/sys/kern/uipc_syscalls.c:715
#16 0xc0511c6e in sendto (td=0xc062b67f,
uap=0xc1015000)
at /usr/src/sys/kern/uipc_syscalls.c:833
#17 0xc05ff737 in syscall (frame=
{tf_fs = 59, tf_es = 59, tf_ds = 59, tf_edi = 672381756,
tf_esi = 134536657, tf_ebp = -1077945788, tf_esp =
-861618844,
tf_ebx = 672417536, tf_edx = 74, tf_ecx = 134541840,
tf_eax =
133, tf_trapno = 12, tf_err = 2, tf_eip = 672270187, tf_cs =
51,
tf_eflags = 534, tf_esp = -1077945820, tf_ss = 59})
at /usr/src/sys/i386/i386/trap.c:1016
#18 0xc05f0b4f in Xint0x80_syscall ()
at /usr/src/sys/i386/i386/exception.s:191
#19 0x00000033 in ?? ()
Previous frame inner to this frame (corrupt stack?)
```

Dmesg:

```
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991,
1992,
1993, 1994
The Regents of the University of California. All rights
reserved.
FreeBSD 7.0-CURRENT #0: Wed Apr 19 13:18:18 EDT
2006
```

```
amistry@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx: /usr/obj/usr/src/sys/LITTLEG
UY Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Transmeta(tm) Crusoe(tm) Processor TM5800
(859.34-MHz
586-class CPU)
Origin = "GenuineTMx86" Id = 0x543 Stepping = 3
Features=0x80893f<FPU,VME,DE,PSE,MSR,CX8,SEP,CMOV,MMX>
real memory = 251527168 (239 MB)
avail memory = 236593152 (225 MB)
Crusoe LongRun support enabled, current mode: 2
<867MHz 1300mV
100%> kbd1 at kbdmux0
acpi0: <FUJ PAULING2> on motherboard
```

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

acpi0: Power Button (fixed)
acpi_ec0: <Embedded Controller: GPE 0> port 0x62,0x66 on
acpi0
Timecounter "ACPI-safe" frequency 3579545 Hz quality
1000
acpi_timer0: <24-bit timer at 3.579545MHz> port
0xff08-0xff0b on
acpi0 cpu0: <ACPI CPU> on acpi0
acpi_throttle0: <ACPI CPU Throttling> on cpu0
pcib0: <ACPI Host-PCI bridge> port 0xcf8-0xcff on acpi0
pci0: <ACPI PCI bus> on pcib0
pci0: <memory, RAM> at device 0.1 (no driver attached)
pci0: <memory, RAM> at device 0.2 (no driver attached)
ohci0: <AcerLabs M5237 (Aladdin-V) USB controller>
mem
0xfc10000-0xfc100ff irq 11 at device 2.0 on pci0
ohci0: [GIANT-LOCKED]
usb0: OHCI version 1.0, legacy support
usb0: <AcerLabs M5237 (Aladdin-V) USB controller> on
ohci0
usb0: USB revision 1.0
usbd_get_string: getting lang failed, using 0
uhub0: <AcerLabs OHCI root hub, class 9/0, rev 1.00/1.00,
addr 1>
on usb0
uhub0: 2 ports with 2 removable, self powered
pcm0: <Acer Labs M5451> port 0x1000-0x10ff mem
0xfc101000-0xfc101fff irq 9 at device 4.0 on pci0
pcm0: <SigmaTel STAC9756/57 AC97 Codec>
pcm0: [GIANT-LOCKED]
pci0: <bridge> at device 6.0 (no driver attached)
isab0: <PCI-ISA bridge> at device 7.0 on pci0
isa0: <ISA bus> on isab0
cbb0: <TI1410 PCI-CardBus Bridge> irq 9 at device 12.0 on
pci0
cardbus0: <CardBus bus> on cbb0
pccard0: <16-bit PCCard bus> on cbb0
atapci0: <AcerLabs M5229 UDMA66 controller> port
0x1f0-0x1f7,0x3f6,0x170-0x177,0x376,0x1400-0x140f at
device 15.0
on pci0
atapci0: using PIO transfers above 137GB as workaround for
48bit
DMA access bug, expect reduced performance
ata0: <ATA channel 0> on atapci0
ata1: <ATA channel 1> on atapci0
rl0: <RealTek 8139 10/100BaseTX> port 0x8000-0x80ff
mem
0xfc102000-0xfc1020ff irq 9 at device 16.0 on pci0
miibus0: <MII bus> on rl0
rlphy0: <RealTek internal media interface> on miibus0

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

```
rlphy0: 10baseT, 10baseT-FDX, 100baseTX,
100baseTX-FDX, auto
rl0: Ethernet address: 00:e0:00:ae:45:08
fwohci0: <Texas Instruments TSB43AB21/A/AI/A-EP>
mem
0xfc102800-0xfc102fff,0xfc104000-0xfc107fff irq 9 at
device 19.0
on pci0
fwohci0: OHCI version 1.10 (ROM=0)
fwohci0: No. of Isochronous channels is 4.
fwohci0: EUI64 00:00:0e:10:00:b0:29:d0
fwohci0: Phy 1394a available S400, 1 ports.
fwohci0: Link S400, max_rec 2048 bytes.
firewire0: <IEEE1394(FireWire) bus> on fwohci0
dcons_crom0: <dcons configuration ROM> on firewire0
dcons_crom0: bus_addr 0xea34000
fwohci0: Initiate bus reset
fwohci0: node_id=0x8800ffc0, gen=1, non
CYCLEMASTER mode
firewire0: 2 nodes, maxhop <= 1, cable IRM = 1
vgapci0: <VGA-compatible display> port 0x1800-0x18ff
mem
0xfd000000-0xfdffffff,0xfc103000-0xfc103fff irq 9 at
device 20.0
on pci0
acpi_video0: <ACPI video extension> on vgapci0
drm0: <Rage Mobility P/M> on vgapci0
info: [drm] Initialized mach64 1.0.0 20020904
acpi_button0: <Power Button> on acpi0
acpi_acad0: <AC Adapter> on acpi0
battery0: <ACPI Control Method Battery> on acpi0
battery1: <ACPI Control Method Battery> on acpi0
acpi_lid0: <Control Method Lid Switch> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1
on
acpi0 atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
atkbd0: [GIANT-LOCKED]
psm0: <PS/2 Mouse> flags 0x3000 irq 12 on atkbdc0
psm0: [GIANT-LOCKED]
psm0: model Generic PS/2 mouse, device ID 0
acpi_fujitsu0: <Fujitsu Function Hotkeys FUJ02B1> on
acpi0
pmtimer0 on isa0
orm0: <ISA Option ROMs> at iomem
0xc0000-0xcffff,0xd0000-0xd0fff
npnid ORM0000 on isa0
sc0: <System console> at flags 0x100 on isa0
sc0: VGA <16 virtual consoles, flags=0x300>
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem
0xa0000-0xbffff
```

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

Re: panic: mutex Giant not owned at /usr/src/sys/cam/cam_xpt.c:4837

```
on isa0
Timecounter "TSC" frequency 859339043 Hz quality 800
Timecounters tick every 10.000 msec
acpi_acad0: acline initialization start
battery0: battery initialization start
battery1: battery initialization start
acpi_acad0: On Line
acpi_acad0: acline initialization done, tried 1 times
battery0: battery initialization done, tried 1 times
ad0: 19077MB <TOSHIBA MK2018GAP M1.42 A> at
ata0-master UDMA66
firewire0: bus manager 1
acd0: CDRW <TOSHIBA DVD-ROM SD-R2212/1F15> at
ata1-master UDMA33
firewire0: New S400 device ID:0000d1008051e6dd
Trying to mount root from ufs:/dev/ad0s2a
WARNING: / was not properly dismounted
WARNING: /tmp was not properly dismounted
WARNING: /usr was not properly dismounted
WARNING: /var was not properly dismounted
battery1: battery initialization failed, giving up
fuse4bsd: version 0.3.0, FUSE ABI 7.5
```

freebsd-current@xxxxxxxxxxx mailing list

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

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