

## Re: "panic: mutex Giant not owned" in do\_execve()

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2005-06/1356.html>

---

**From:** John Baldwin ([jhb\\_at\\_FreeBSD.org](mailto:jhb_at_FreeBSD.org))

**Date:** 06/27/05

To: [freebsd-current@freebsd.org](mailto:freebsd-current@freebsd.org)

Date: Mon, 27 Jun 2005 16:56:14 -0400

On Monday 20 June 2005 04:47 pm, Jeff Roberson wrote:

```
> On Fri, 17 Jun 2005, Kris Kennaway wrote:
> > quad e450 running up-to-date -current:
> >
> > panic: mutex Giant not owned at ../../kern/kern_mutex.c:299
> > cpuid = 0
> > KDB: enter: panic
> > [thread pid 52851 tid 100456 ]
> > Stopped at kdb_enter+0x3c: ta %xcc, 1
> > db> wh
> > Tracing pid 52851 tid 100456 td 0xffff80077c61560
> > panic() at panic+0x16c
> > _mtx_assert() at _mtx_assert+0x6c
> > _mtx_unlock_flags() at _mtx_unlock_flags+0x68
> > do_execve() at do_execve+0xa0c
>
> Can you tell me what code is at do_execve+0xa0c?
```

It's down below. It's the VFS\_UNLOCK\_GIANT() after the #ifdef MAC stuff:

```
> > kern_execve() at kern_execve+0x7c
> > execve() at execve+0x38
> > syscall() at syscall+0x2d4
> > -- reserved %o7=0 --
> > userland() at 0x40223400
> > user trace: trap %o7=0
> > pc 0x40223400, sp 0x7fdffffd021
> > done
> >
> > #12 0x00000000c01525cc in do_execve (td=0xffff80077c61560, args=0xc,
> > mac_p=0x0) at ../../kern/kern_exec.c:789
> > #13 0x00000000c0151b3c in kern_execve (td=0xffff80077c61560,
> > args=0xeea6f670, mac_p=0x0) at
> > ../../kern/kern_exec.c:250
> > #14 0x00000000c0151a78 in execve (td=0xffff80077c61560, uap=0xeea6f8c0)
> > at ../../kern/kern_exec.c:185
> > #15 0x00000000c02f3cd4 in syscall (tf=0xeea6f880) at
```

freebsd-current: Re: "panic: mutex Giant not owned" in do\_execve()

```
> > ../../sparc64/sparc64/trap.c:592
> > (kgdb) frame 12
> > #12 0x00000000c01525cc in do_execve (td=0xffff80077c61560, args=0xc,
> > mac_p=0x0) at ../../kern/kern_exec.c:789
> > 789 VFS_UNLOCK_GIANT(vfslocked);
> > (kgdb) list
> > 784 #ifdef MAC
> > 785 mac_execve_exit(imgp);
> > 786 if (interlabel != NULL)
> > 787 mac_vnode_label_free(interlabel);
> > 788 #endif
> > 789 VFS_UNLOCK_GIANT(vfslocked);
> > 790 return (error);
> > 791 }
> > 792
> > 793 int
```

See, line 789 here.

--

John Baldwin <jhb@FreeBSD.org> <>< <http://www.FreeBSD.org/~jhb/>  
"Power Users Use the Power to Serve" = <http://www.FreeBSD.org>

---

freebsd-current@freebsd.org mailing list

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

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