

kldload(8) might panic

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2003-07/1125.html>

From: Rene Ladan (r.c.ladan_at_student.tue.nl)

Date: 07/18/03

Date: Fri, 18 Jul 2003 19:37:32 +0200
To: freebsd-current@freebsd.org

Hi,

on my 5.1R-box, I sometimes get the below panic message when loading a module into the kernel with kldload(8).

It seems that some part of the linker reports a bogus value for the required memory. Other times loading modules works fine.

Rene

Script started on Fri Jul 18 19:35:09 2003

rene@n188:/usr/home/rene\$ uname -a

FreeBSD n188.dial.tue.nl 5.1-RELEASE FreeBSD 5.1-RELEASE #0: Thu Jul 17 15:34:28 CEST 2003

root@atmosphere.local:/usr/src-releng51/sys/i386/compile/RENE_2003-07-17 i386

rene@n188:/usr/home/rene\$ cat /usr/tmp/gd bk.0

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:

panic: kmem_malloc(42766336): kmem_map too small: 55050240 total allocated

panic: from debugger

Uptime: 8h50m15s

Dumping 191 MB

ata0: resetting devices ..

done

16 32 48 64 80 96 112 128 144 160 176

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

Loaded symbols for /boot/kernel/vesa.ko

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

Loaded symbols for /boot/kernel/acpi.ko

freebsd-current: kldload(8) might panic

```
Reading symbols from /boot/kernel/blank_saver.ko...done.
Loaded symbols for /boot/kernel/blank_saver.ko
Reading symbols from /boot/kernel/umodem.ko...done.
Loaded symbols for /boot/kernel/umodem.ko
#0 doadump () at ../../kern/kern_shutdown.c:238
238 ../../kern/kern_shutdown.c: No such file or directory.
   in ../../kern/kern_shutdown.c
(kgdb) bt full
#0 doadump () at ../../kern/kern_shutdown.c:238
No locals.
#1 0xc024eafd in boot (howto=260) at ../../kern/kern_shutdown.c:370
No locals.
#2 0xc024ef48 in panic () at ../../kern/kern_shutdown.c:543
   td = (struct thread *) 0xc226c000
   bootopt = 260
   newpanic = 0
   buf = "from debugger\0766336): kmem_map too small: 55050240 total allocated", '\0' <repeats 188
times>
#3 0xc0130b75 in db_panic () at ../../ddb/db_command.c:448
No locals.
#4 0xc0130ad2 in db_command (last_cmdp=0xc042b5e0, cmd_table=0x0,
   aux_cmd_tablep=0xc0426f38, aux_cmd_tablep_end=0xc0426f3c)
   at ../../ddb/db_command.c:346
   cmd = (struct command *) 0xc03eccb4
   t = 0
   modif =
"\08ÏÏ\bâ9ÀÐß9ÀØÐ9À\200wJÀ`äHÀæGÀ\b\217KÀP8ÏÏîP9À°P9À9ð(À`äHÀx\0\0\0æGÀ\b\217KÀx8ÏÏ\|a\023À°.
   addr = -1069890249
   count = -1
   have_addr = 0
   result = 0
#5 0xc0130c16 in db_command_loop () at ../../ddb/db_command.c:470
No locals.
#6 0xc013446b in db_trap (type=3, code=0) at ../../ddb/db_trap.c:72
   bkpt = 0
#7 0xc03ac205 in kdb_trap (type=3, code=0, regs=0xcfcc3974)
   at ../../i386/i386/db_interface.c:170
   ef = 70
   ddb_mode = 1
#8 0xc03c082c in trap (frame=
   {tf_fs = -1069875176, tf_es = 16, tf_ds = -1068826608, tf_edi = -1037647872, tf_esi = 1, tf_ebp =
-808699456, tf_isp = -808699488, tf_ebx = 0, tf_edx = 0, tf_ecx = 0, tf_eax = -1069890250, tf_trapno = 3,
tf_err = 0, tf_eip = -1069890249, tf_cs = 8, tf_eflags = 663, tf_esp = -1069413180, tf_ss = -1069477935})
   at ../../i386/i386/trap.c:593
   td = (struct thread *) 0xc226c000
   p = (struct proc *) 0xc226bd20
   sticks = 1
   i = 0
   ucode = 0
   type = 3
   code = 0
```

freebsd-current: kldload(8) might panic

```
    eva = 0
#9 0xc03ae1ee in calltrap () at {standard input}:96
No locals.
#10 0xc024ee9b in panic (fmt=0x0) at ../../kern/kern_shutdown.c:527
    td = (struct thread *) 0xc226c000
    bootopt = 256
    newpanic = 1
    buf = "from debugger\0766336): kmem_map too small: 55050240 total allocated", '\0' <repeats 188
times>
#11 0xc035c6ea in kmem_malloc (map=0xc082f0b0, size=42766336, flags=2)
    at ../../vm/vm_kern.c:339
    offset = 3224838192
    i = 3257833656
    entry = (struct vm_map_entry *) 0xc0372440
    addr = 3234832384
    m = (struct vm_page *) 0x0
    pflags = -1070128770
#12 0xc0370e3d in page_alloc (zone=0x0, bytes=0, pflag=0x0, wait=0)
    at ../../vm/uma_core.c:803
    p = (void *) 0x0
#13 0xc037327e in uma_large_malloc (size=42766336, wait=2)
    at ../../vm/uma_core.c:2034
    mem = (void *) 0x0
    slab = (struct uma_slab *) 0xc22e98b8
    flags = 2 '\002'
#14 0xc02413c1 in malloc (size=42766336, type=0xc045cd20, flags=2)
    at ../../kern/kern_malloc.c:240
    indx = 42766336
    va = 0xc226c000 " ½&Â"
    zone = (struct uma_zone *) 0xcfcc3b44
    ksp = (struct malloc_type *) 0xc045cd20
#15 0xc0275ffc in kmupetext (nhighpc=3289623160)
    at ../../kern/subr_prof.c:109
    np = {state = 3, kcount = 0xc241dfe8, kcountsize = 33581392,
froms = 0xc32fe6e8, fromssize = 8395348, tos = 0xc235e000, tossize = 786408,
tolimit = 65534, lowpc = 3222460384, highpc = 3289623168,
textsize = 67162784, hashfraction = 8, profrate = 497559752,
cputime_count = 0xc256f050, cputime_overhead = 50,
mcount_count = 0xc24ea7f8, mcount_overhead = 141, mcount_post_overhead = 53,
mcount_pre_overhead = 138, mexitcount_count = 0xc24ea8d0,
mexitcount_overhead = 83, mexitcount_post_overhead = 10,
mexitcount_pre_overhead = 123, histcounter_type = 0}
    p = (struct gmonparam *) 0xc045cdc0
    cp = 0xc1ff5000 "\177ELF\001\001\001\t"
#16 0xc026467b in link_elf_load_file (cls=0xc045bf90,
filename=0xc2057020 "/boot/kernel/umodem.ko", result=0x0)
    at ../../kern/link_elf.c:753
    nd = {ni_dirp = 0xc2057020 "/boot/kernel/umodem.ko",
ni_segflg = UIO_SYSSPACE, ni_startdir = 0x0, ni_rootdir = 0xc229ddb0,
ni_topdir = 0x0, ni_vp = 0xc3d9b36c, ni_dvp = 0xc3d7c920, ni_pathlen = 1,
ni_next = 0xc1faf416 "", ni_loopcnt = 0, ni_cnd = {cn_nameiop = 0,
```

freebsd-current: kldload(8) might panic

```
cn_flags = 2146372, cn_thread = 0xc226c000, cn_cred = 0xc38f1b00,
cn_pnbuf = 0xc1faf400 "/boot/kernel/umodem.ko",
cn_nameptr = 0xc1faf40d "umodem.ko", cn_namelen = 9, cn_consume = 0} }
  td = (struct thread *) 0xc226c000
  hdr = (struct {...} *) 0xc1ff5000
  firstpage = 0xc1ff5000 "\177ELF\001\001\001\t"
  nbytes = 4096
  i = 2
  phdr = (struct {...} *) 0x0
  phlimit = (struct {...} *) 0x0
  segs = {0xc1ff5034, 0xc1ff5054}
  nsegs = 0
  phdyn = (struct {...} *) 0xc1ff5074
  mapbase = 0xc4139000 "\177ELF\001\001\001\t"
  mapsize = 12288
  base_vaddr = 0
  base_vlimit = 0
  error = 0
  resid = 0
  flags = 1
  ef = (struct elf_file *) 0xc2058d00
  lf = (struct linker_file *) 0xc2058d00
  shdr = (struct {...} *) 0x0
  symtabindex = 0
  symstrindex = 0
  symcnt = 0
  strcnt = 0
#17 0xc023f1da in LINKER_LOAD_FILE (cls=0xc045bf90, filename=0x0, result=0x0)
  at linker_if.h:88
  _m = (int (*)(void)) 0
#18 0xc023bc33 in linker_load_file (
  filename=0xc2057020 "/boot/kernel/umodem.ko", result=0xcfcc3c94)
  at ../../kern/kern_linker.c:346
  lc = (struct linker_class *) 0xc0d05028
  lf = (struct linker_file *) 0x0
  foundfile = 0
  error = -1069170800
#19 0xc023e947 in linker_load_module (kldname=0xc045bf90 "pë@À@;EÀÈ",
  modname=0xc2057020 "/boot/kernel/umodem.ko", parent=0x0, verinfo=0x0,
  lfpp=0xcfcc3cc0) at ../../kern/kern_linker.c:1669
  lfdep = (struct linker_file *) 0xc02c66b0
  filename = 0x0
  pathname = 0xc045bf90 "pë@À@;EÀÈ"
  error = -1060089816
#20 0xc023caae in kldload (td=0xc2057020, uap=0x0)
  at ../../kern/kern_linker.c:772
  kldname = 0x0
  modname = 0x0
  pathname = 0xc045bf90 "pë@À@;EÀÈ"
  lf = (struct linker_file *) 0xc226c000
  error = -1060089816
```

freebsd-current: kldload(8) might panic

```
#21 0xc03c11fa in syscall (frame=  
  {tf_fs = 47, tf_es = 47, tf_ds = 47, tf_edi = 0, tf_esi = -1077937068, tf_ebp = -1077937112, tf_isp =  
-808698508, tf_ebx = 0, tf_edx = 134562984, tf_ecx = 0, tf_eax = 304, tf_trapno = 12, tf_err = 2, tf_eip =  
134513919, tf_cs = 31, tf_eflags = 531, tf_esp = -1077937156, tf_ss = 47})  
  at ../../i386/i386/trap.c:1021  
  params = 0xbfbffc00---Can't read userspace from dump, or kernel process---
```

```
rene@n188:/usr/home/rene$ cat /usr/tmp/gd bk.1
```

```
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:
```

```
---
```

```
panic: kmem_malloc(29892608): kmem_map too small: 54829056 total allocated
```

```
panic: from debugger
```

```
Uptime: 1d1h20m47s
```

```
Dumping 191 MB
```

```
ata0: resetting devices ..
```

```
done
```

```
16 32 48 64 80 96 112 128 144 160 176
```

```
---
```

```
Reading symbols from /boot/kernel/vesa.ko...done.
```

```
Loaded symbols for /boot/kernel/vesa.ko
```

```
Reading symbols from /boot/kernel/blank_saver.ko...done.
```

```
Loaded symbols for /boot/kernel/blank_saver.ko
```

```
Reading symbols from /boot/kernel/apm.ko...done.
```

```
Loaded symbols for /boot/kernel/apm.ko
```

```
#0 doadump () at ../../kern/kern_shutdown.c:238
```

```
238 ../../kern/kern_shutdown.c: No such file or directory.
```

```
  in ../../kern/kern_shutdown.c
```

```
(kgdb) bt full
```

```
#0 doadump () at ../../kern/kern_shutdown.c:238
```

```
No locals.
```

```
#1 0xc024f9fd in boot (howto=260) at ../../kern/kern_shutdown.c:370
```

```
No locals.
```

```
#2 0xc024fe48 in panic () at ../../kern/kern_shutdown.c:543
```

```
  td = (struct thread *) 0xc23834c0
```

```
  bootopt = 260
```

```
  newpanic = 0
```

```
  buf = "from debugger(0892608): kmem_map too small: 54829056 total allocated", '\0' <repeats 188  
times>
```

```
#3 0xc0130a75 in db_panic () at ../../ddb/db_command.c:448
```

```
No locals.
```

```
#4 0xc01309d2 in db_command (last_cmdp=0xc04295e0, cmd_table=0x0,
```

```
  aux_cmd_tablep=0xc0424f40, aux_cmd_tablep_end=0xc0424f44)
```

```
  at ../../ddb/db_command.c:346
```

```
kldload(8) might panic
```

freebsd-current: kldload(8) might panic

```
cmd = (struct command *) 0xc03eb214
t = 0
modif =
"\001\bñ9ÀÐí9ÀØí9ÀàUJÀÀÂHÀ@DGÀèiKÀPØÏíí9À°í9À9\001)ÀÀÂHÀx\0\0\0@DGÀèiKÀxØÏí\à.\023À°-\02
addr = -1069896185
count = -1
have_addr = 0
result = 0
#5 0xc0130b16 in db_command_loop () at ../../ddb/db_command.c:470
No locals.
#6 0xc013436b in db_trap (type=3, code=0) at ../../ddb/db_trap.c:72
bkpt = 0
#7 0xc03aaad5 in kdb_trap (type=3, code=0, regs=0xcfc974)
at ../../i386/i386/db_interface.c:170
ef = 70
ddb_mode = 1
#8 0xc03bf0fc in trap (frame=
{tf_fs = -808583144, tf_es = -1070989296, tf_ds = -1070989296, tf_edi = -1036503872, tf_esi = 1,
tf_ebp = -808527424, tf_esp = -808527456, tf_ebx = 0, tf_edx = 0, tf_ecx = 32, tf_eax = -1069896186,
tf_trapno = 3, tf_err = 0, tf_eip = -1069896185, tf_cs = 8, tf_eflags = 663, tf_esp = -1069421272, tf_ss =
-1069484321}) at ../../i386/i386/trap.c:593
td = (struct thread *) 0xc23834c0
p = (struct proc *) 0xc23825a0
sticks = 3317747509
i = 0
ucode = 0
type = 3
code = 0
eva = 0
#9 0xc03acabe in calltrap () at {standard input}:96
No locals.
#10 0xc024fd9b in panic (fmt=0x0) at ../../kern/kern_shutdown.c:527
td = (struct thread *) 0xc23834c0
bootopt = 256
newpanic = 1
buf = "from debugger(0892608): kmem_map too small: 54829056 total allocated", '\0' <repeats 188
times>
#11 0xc035d5ea in kmem_malloc (map=0xc082f0b0, size=29892608, flags=2)
at ../../vm/vm_kern.c:339
offset = 3224842032
i = 3258221552
entry = (struct vm_map_entry *) 0xc0373340
addr = 3234832384
m = (struct vm_page *) 0x0
pflags = -1070124930
#12 0xc0371d3d in page_alloc (zone=0x0, bytes=0, pflag=0x0, wait=0)
at ../../vm/uma_core.c:803
p = (void *) 0x0
#13 0xc037417e in uma_large_malloc (size=29892608, wait=2)
at ../../vm/uma_core.c:2034
mem = (void *) 0x0
```

kldload(8) might panic

freebsd-current: kldload(8) might panic

```
slab = (struct uma_slab *) 0xc23483f0
flags = 2 '\002'
#14 0xc02422c1 in malloc (size=29892608, type=0xc045ae20, flags=2)
at ../../kern/kern_malloc.c:240
    indx = 29892608
    va = 0xc23834c0 "%8Â"
    zone = (struct uma_zone *) 0xcfcdb44
    ksp = (struct malloc_type *) 0xc045ae20
#15 0xc0276efc in kmupetext (nhighpc=3269024940)
at ../../kern/subr_prof.c:109
    np = {state = 3, kcount = 0xc3746fe8, kcountsize = 23282408,
froms = 0xc469a2d0, fromssize = 5820602, tos = 0xc3687000, tossize = 786408,
tolimit = 65534, lowpc = 3222460128, highpc = 3269024944,
textsize = 46564816, hashfraction = 8, profrate = 497558844,
cputime_count = 0xc3897380, cputime_overhead = 50,
mcount_count = 0xc3813ff8, mcount_overhead = 141, mcount_post_overhead = 52,
mcount_pre_overhead = 139, mexitcount_count = 0xc38140d0,
mexitcount_overhead = 83, mexitcount_post_overhead = 10,
mexitcount_pre_overhead = 123, histcounter_type = 0}
    p = (struct gmonparam *) 0xc045aec0
    cp = 0xc2274000 "\177ELF\001\001\001\t"
#16 0xc026557b in link_elf_load_file (cls=0xc045a090,
filename=0xc2109b00 "/boot/kernel/apm.ko", result=0x0)
at ../../kern/link_elf.c:753
    nd = {ni_dirp = 0xc2109b00 "/boot/kernel/apm.ko",
ni_segflg = UIO_SYSSPACE, ni_startdir = 0x0, ni_rootdir = 0xc2287db0,
ni_topdir = 0x0, ni_vp = 0xc2c6a36c, ni_dvp = 0xc2c816d8, ni_pathlen = 1,
ni_next = 0xc1fa5813 "", ni_loopcnt = 0, ni_cnd = {cn_nameiop = 0,
cn_flags = 2146372, cn_thread = 0xc23834c0, cn_cred = 0xc223b900,
cn_pnbuf = 0xc1fa5800 "/boot/kernel/apm.ko",
cn_nameptr = 0xc1fa580d "apm.ko", cn_namelen = 6, cn_consume = 0}}
    td = (struct thread *) 0xc23834c0
    hdr = (struct {...} *) 0xc2274000
    firstpage = 0xc2274000 "\177ELF\001\001\001\t"
    nbytes = 4096
    i = 2
    phdr = (struct {...} *) 0x0
    phlimit = (struct {...} *) 0x0
    segs = {0xc2274034, 0xc2274054}
    nsegs = 0
    phdyn = (struct {...} *) 0xc2274074
    mapbase = 0xc2d92000 "\177ELF\001\001\001\t"
    mapsize = 20480
    base_vaddr = 0
    base_vlimit = 0
    error = 0
    resid = 0
    flags = 1
    ef = (struct elf_file *) 0xc2492400
    lf = (struct linker_file *) 0xc2492400
    shdr = (struct {...} *) 0x0
```

freebsd-current: kldload(8) might panic

```
symtabindex = 0
symstrindex = 0
symcnt = 0
strcnt = 0
#17 0xc02400da in LINKER_LOAD_FILE (cls=0xc045a090, filename=0x0, result=0x0)
at linker_if.h:88
    _m = (int (*)(void)) 0
#18 0xc023cb33 in linker_load_file (filename=0xc2109b00 "/boot/kernel/apm.ko",
result=0xcfc94) at ../../kern/kern_linker.c:346
    lc = (struct linker_class *) 0xc0d05028
    lf = (struct linker_file *) 0x0
    foundfile = 0
    error = -1069178736
#19 0xc023f847 in linker_load_module (kldname=0xc045a090 "\fÓ@À@ EÀÈ",
modname=0xc2109b00 "/boot/kernel/apm.ko", parent=0x0, verinfo=0x0,
lfpp=0xcfc94) at ../../kern/kern_linker.c:1669
    lfdep = (struct linker_file *) 0xc02c75b0
    filename = 0x0
    pathname = 0xc045a090 "\fÓ@À@ EÀÈ"
    error = -1060089816
#20 0xc023d9ae in kldload (td=0xc2109b00, uap=0x0)
at ../../kern/kern_linker.c:772
    kldname = 0x0
    modname = 0x0
    pathname = 0xc045a090 "\fÓ@À@ EÀÈ"
    lf = (struct linker_file *) 0xc23834c0
    error = -1060089816
#21 0xc03bfaca in syscall (frame=
{tf_fs = 47, tf_es = 47, tf_ds = 47, tf_edi = 0, tf_esi = -1077937064, tf_ebp = -1077937108, tf_isp =
-808526476, tf_ebx = 0, tf_edx = 134562984, tf_ecx = 0, tf_eax = 304, tf_trapno = 12, tf_err = 2, tf_eip =
134513919, tf_cs = 31, tf_eflags = 531, tf_esp = -1077937156, tf_ss = 47})
at ../../i386/i386/trap.c:1021
    params = 0xbfbffc00---Can't read userspace from dump, or kernel process---
rene@n188:/usr/home/rene$ exit
```

Script done on Fri Jul 18 19:36:10 2003

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"