

bug: hid module crashed

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-04/0382.html>

From: Tomas Vinar (tvinar_at_math.uwaterloo.ca)

Date: 04/02/04

Date: Thu, 1 Apr 2004 19:52:18 -0500 (EST)

To: linux-kernel@vger.kernel.org

Linux proteome 2.4.22-openmosix-2bif #1 SMP Sun Jan 4 16:12:36 EST 2004

i686 unknown

Gnu C 2.95.4

Gnu make 3.79.1

util-linux 2.11n

mount 2.11n

modutils 2.4.21

e2fsprogs 1.27

PPP 2.4.1

Linux C Library 2.2.5

Dynamic linker (ld) 2.2.5

Procps 2.0.7

Net-tools 1.60

Console-tools 0.2.3

Sh-utils 2.0.11

Modules Loaded hid input usb-ohci usbcore nfs lockd sunrpc bcm5700

af_packet rtc unix

ksymoops 2.4.5 on i686 2.4.22-openmosix-2bif. Options used

-V (default)

-k /proc/ksyms (default)

-l /proc/modules (default)

-o /lib/modules/2.4.22-openmosix-2bif/ (default)

-m /boot/System.map-2.4.22-openmosix-2bif (default)

Warning: You did not tell me where to find symbol information. I will assume that the log matches the kernel and modules that are running right now and I'll use the default options above for symbol resolution. If the current kernel and/or modules do not match the log, you can get more accurate output by telling me the kernel version and where to find map, modules, ksyms etc. ksymoops -h explains the options.

Warning (compare_ksyms_lsm): module hid is in lsm but not in ksyms, probably no symbols exported

kernel BUG at pipe.c:136!

invalid operand: 0000

bug: hid module crashed

Linux-Kernel: bug: hid module crashed

```
CPU: 0
EIP: 0010:[<c01523a6>] Not tainted
Using defaults from ksymoops -t elf32-i386 -a i386
EFLAGS: 00010206
eax: f2d4bb80 ebx: f2d4bb80 ecx: 00000000 edx: 00000001
esi: d6055100 edi: 00003000 ebp: c90c8000 esp: c90c9f80
ds: 0018 es: 0018 ss: 0018
Process dpkg-deb (pid: 15946, stackpage=c90c9000)
Stack: 00000000 e6192d00 ffffffff 00004000 d605516c ffffffff 00001000 c014862b
       e6192d00 08067c58 00004000 e6192d20 c90c8000 00001000 080759d8 bfffe9ac
       c010ac28 00000000 08066c58 00004000 00001000 080759d8 bfffe9ac 00000003
Call Trace: [<c014862b>] [<c010ac28>]
Code: 0f 0b 88 00 fd 36 2b c0 e9 fa fd ff ff b9 01 00 00 00 ba 01
>>EIP; c01523a6 <pipe_read+272/2d0> <=====
>>eax; f2d4bb80 <_end+32945810/38410cf0>
>>ebx; f2d4bb80 <_end+32945810/38410cf0>
>>esi; d6055100 <_end+15c4ed90/38410cf0>
>>edi; 00003000 Before first symbol
>>ebp; c90c8000 <_end+8cc1c90/38410cf0>
>>esp; c90c9f80 <_end+8cc3c10/38410cf0>
Trace; c014862b <sys_read+8f/100>
Trace; c010ac28 <local_syscall+7/13>
Code; c01523a6 <pipe_read+272/2d0>
00000000 <_EIP>:
Code; c01523a6 <pipe_read+272/2d0> <=====
 0: 0f 0b ud2a <=====
Code; c01523a8 <pipe_read+274/2d0>
 2: 88 00 mov %al,(%eax)
Code; c01523aa <pipe_read+276/2d0>
 4: fd std
Code; c01523ab <pipe_read+277/2d0>
 5: 36 ss
Code; c01523ac <pipe_read+278/2d0>
 6: 2b c0 sub %eax,%eax
Code; c01523ae <pipe_read+27a/2d0>
 8: e9 fa fd ff ff jmp fffffe07 <_EIP+0xfffffe07> c01521ad <pipe_read+79/2d0>
Code; c01523b3 <pipe_read+27f/2d0>
 d: b9 01 00 00 00 mov $0x1,%ecx
Code; c01523b8 <pipe_read+284/2d0>
12: ba 01 00 00 00 mov $0x1,%edx
kernel BUG at base.c:914!
invalid operand: 0000
CPU: 0
EIP: 0010:[<c0191db0>] Not tainted
EFLAGS: 00010286
eax: 0000000d ebx: f5a97800 ecx: 00000001 edx: 00000001
esi: 00000000 edi: f899f820 ebp: f899f840 esp: d3f4bee8
ds: 0018 es: 0018 ss: 0018
Process modprobe (pid: 29411, stackpage=d3f4b000)
Stack: c02c0003 c02bffe6 c02bffd6 f5a97800 f5a97800 c0192db4 f5a97800 f5ad9f00
       f5a97800 f5b3e680 f899c23e f5a97800 f5b3e680 f899dbf6 f5b3e680 f5caa000
       f899becf f5caa000 f69385c0 f89811e6 f66b2800 f5caa000 f653ef10 00000001
Call Trace: [<c0192db4>] [<f899c23e>] [<f899dbf6>] [<f899becf>] [<f89811e6>]
           [<f899f820>] [<f8981192>] [<f899f820>] [<f898fee8>] [<f899f820>] [<f8990460>]
           [<f89812bf>] [<f899f820>] [<f899bf1b>] [<f899f820>] [<c0124b23>] [<c012378a>]
           [<c010ac28>]
Code: 0f 0b 92 03 11 00 2c c0 83 c4 10 f0 ff 4b 04 0f 94 c0 84 c0
>>EIP; c0191db0 <devfs_put+30/e8> <=====
>>ebx; f5a97800 <_end+35691490/38410cf0>
>>edi; f899f820 <END_OF_CODE+9039/????>
>>ebp; f899f840 <END_OF_CODE+9059/????>
>>esp; d3f4bee8 <_end+13b45b78/38410cf0>
```

bug: hid module crashed

Linux-Kernel: bug: hid module crashed

```
Trace; c0192db4 <devfs_unregister+30/38>
Trace; f899c23e <.&data.end+5a57/????>
Trace; f899dbf6 <.&data.end+740f/????>
Trace; f899becf <.&data.end+56e8/????>
Trace; f89811e6 <[usbcore]usb_drivers_purge+92/e0>
Trace; f899f820 <END_OF_CODE+9039/????>
Trace; f8981192 <[usbcore]usb_drivers_purge+3e/e0>
Trace; f899f820 <END_OF_CODE+9039/????>
Trace; f898fee8 <[usbcore]usb_bus_list+0/18>
Trace; f899f820 <END_OF_CODE+9039/????>
Trace; f8990460 <[usbcore]usb_bus_list_lock+0/14>
Trace; f89812bf <[usbcore]usb_deregister+8b/ac>
Trace; f899f820 <END_OF_CODE+9039/????>
Trace; f899bf1b <.&data.end+5734/????>
Trace; f899f820 <END_OF_CODE+9039/????>
Trace; c0124b23 <free_module+17/b0>
Trace; c012378a <sys_delete_module+126/23c>
Trace; c010ac28 <local_syscall+7/13>
Code; c0191db0 <devfs_put+30/e8>
00000000 <_EIP>:
Code; c0191db0 <devfs_put+30/e8> <=====
  0:  0f 0b                ud2a          <=====
Code; c0191db2 <devfs_put+32/e8>
  2:  92                    xchg   %eax,%edx
Code; c0191db3 <devfs_put+33/e8>
  3:  03 11                add    (%ecx),%edx
Code; c0191db5 <devfs_put+35/e8>
  5:  00 2c c0            add    %ch,(%eax,%eax,8)
Code; c0191db8 <devfs_put+38/e8>
  8:  83 c4 10            add    $0x10,%esp
Code; c0191dbb <devfs_put+3b/e8>
  b:  f0 ff 4b 04        lock decl 0x4(%ebx)
Code; c0191dbf <devfs_put+3f/e8>
  f:  0f 94 c0            sete   %al
Code; c0191dc2 <devfs_put+42/e8>
 12:  84 c0            test  %al,%al
2 warnings issued.  Results may not be reliable.
```

Tomas Vinar, University of Waterloo graduate student
E-mail: tvinar@math.uwaterloo.ca
Office: DC3542, (519)888-4567 ext. 3564
Home phone: (519)746-7632

-
To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to majordomo@vger.kernel.org
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>