

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btdelconn

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2008-02/msg08106.html>

- *From:* Barnaby <diannibd@xxxxxxxxxx>
 - *Date:* Sat, 16 Feb 2008 00:16:18 -0500
-

On Fri, Feb 15, 2008 at 6:15 PM, Dave Young <hidave.darkstar@xxxxxxxxxx> wrote:

On Fri, Feb 15, 2008 at 8:04 AM, Barnaby <diannibd@xxxxxxxxxx> wrote:

> Answers at the bottom..

>

>

>

> On 2/13/08, Dave Young <hidave.darkstar@xxxxxxxxxx> wrote:

>> On Feb 8, 2008 12:57 AM, Barnaby <diannibd@xxxxxxxxxx> wrote:

>>> Hello Dave,

>>>

>>> Add someone to cc-list

>>>

>>>

>>>>

>>>> Got your name and email from the 2.6.24-git16 changelog.

>>>>

>>>> I get these Oops when suspending or doing..

>>>>

>>>> echo disable > /proc/acpi/ibm/bluetooth

>>>> or

>>>> echo 0 > /sys/devices/platform/thinkpad_acpi/bluetooth_enable

>>>>

>>>> # -----

>>>>

>>>> Feb 7 09:19:47 BUG: unable to handle kernel NULL pointer dereference

>>>> at 00000008

>>>> Feb 7 09:19:47 IP: [

>>>> Feb 7 09:19:47 *pde = 00000000

>>>> Feb 7 09:19:47 Oops: 0000 [#1] PREEMPT

>>>> Feb 7 09:19:47 Modules linked in: xt_tcpudp hidp l2cap snd_seq

>>>> snd_seq_device snd_pcm_oss snd_mixer_oss sr_mod cdrom iptable_filter

>>>> iptable_nat nf_conntrack_ipv4 iptable_mangle ipt_LOG xt_state ipt_ttl

>>>> ipt_MASQUERADE nf_nat nf_conntrack xt_DSCP ip_tables x_tables usbhid

>>>> ipw2200 ieee80211 ieee80211_crypt thinkpad_acpi backlight acpi_cpufreq

>>>> radeon drm intel_agp agpgart snd_intel8x0 snd_ac97_codec ac97_bus

>>>> snd_pcm snd_timer snd soundcore snd_page_alloc button

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btldelconn

```
>>> thermal processor hci_usb bluetooth
>>> Feb 7 09:19:47
>>> Feb 7 09:19:47 Pid: 1412, comm: btldelconn Not tainted (2.6.24-git16 #1)
>>> Feb 7 09:19:47 EIP: 0060:[<c0183188>] EFLAGS: 00010246 CPU: 0
>>> Feb 7 09:19:47 EIP is at sysfs_move_dir+0x16/0x1ab
>>> Feb 7 09:19:47 EAX: c039476c EBX: f7dd0480 ECX: f6da9f58 EDX: f7dd0480
>>> Feb 7 09:19:47 ESI: 00000000 EDI: f5ea0c40 EBP: ffffffff4 ESP: f6da9f30
>>> Feb 7 09:19:47 DS: 007b ES: 007b FS: 0000 GS: 0000 SS: 0068
>>> Feb 7 09:19:47 Process btldelconn (pid: 1412, ti=f6da8000
>>> task=f6fd1550 task.ti=f6da8000)
>>> Feb 7 09:19:47 Stack: f56f4ea4 f7dd0480 f5ea0c40 f56f4ea4 f7dd0480
>>> f5ea0c40 ffffffff4 c01c71a0
>>> Feb 7 09:19:47 f5ea0800 c034a793 f5ea0c40 f5ea0800 f5ea0800 00000000
>>> f56f4e3c 00000000
>>> Feb 7 09:19:47 00000000 f7dd0480 c0219d48 f56f4ea4 ffffffff4 f56f4e3c
>>> f5fc7c88 f5fc7c00
>>> Feb 7 09:19:47 Call Trace:
>>> Feb 7 09:19:47 [<c01c71a0>] kobject_move+0x9e/0xeb
>>> Feb 7 09:19:47 [<c0219d48>] device_move+0x41/0xdf
>>> Feb 7 09:19:47 [<f88657f6>] del_conn+0x0/0x43 [bluetooth]
>>> Feb 7 09:19:47 [<f8865807>] del_conn+0x11/0x43 [bluetooth]
>>> Feb 7 09:19:47 [<c012339b>] run_workqueue+0x83/0x10e
>>> Feb 7 09:19:47 [<c0123996>] worker_thread+0x0/0xb5
>>> Feb 7 09:19:47 [<c0123a41>] worker_thread+0xab/0xb5
>>> Feb 7 09:19:47 [<c0125d5e>] autoremove_wake_function+0x0/0x2d
>>> Feb 7 09:19:47 [<c0125caa>] kthread+0x36/0x5c
>>> Feb 7 09:19:47 [<c0125c74>] kthread+0x0/0x5c
>>> Feb 7 09:19:47 [<c01047cb>] kernel_thread_helper+0x7/0x10
>>> Feb 7 09:19:47 =====
>>> Feb 7 09:19:47 Code: ff b8 6c 47 39 c0 e8 64 f1 15 00 89 f0 83 c4 10
>>> 5b 5e 5f 5d c3 55 57 56 53 89 d3 83 ec 0c 8b 70 1c b8 6c 47 39 c0 e8
>>> 3a f1 15 00 <8b> 56 08 85 d2 75 04 0f 0b eb fe 8b 5b 1c b8 a0 47 39 c0
>>> 85 db
>>> Feb 7 09:19:47 EIP: [<c0183188>] sysfs_move_dir+0x16/0x1ab SS:ESP
>>> 0068:f6da9f30
>>> Feb 7 09:19:47 ---[ end trace e0c3df2b167f1367 ]---
>>> Feb 7 09:27:44 usb 4-1: new full speed USB device using uhci_hcd and address 4
>>> Feb 7 09:27:44 usb 4-1: configuration #1 chosen from 1 choice
>>> Feb 7 09:28:06 BUG: unable to handle kernel NULL pointer dereference
>>> at 00000020
>>> Feb 7 09:28:06 IP: [<c0182a99>] sysfs_addrm_start+0x1e/0x7a
>>> Feb 7 09:28:06 *pde = 00000000
>>> Feb 7 09:28:06 Oops: 0000 [#2] PREEMPT
>>> Feb 7 09:28:06 Modules linked in: xt_tcpudp hidp l2cap snd_seq
>>> snd_seq_device snd_pcm_oss snd_mixer_oss sr_mod cdrom iptable_filter
>>> iptable_nat nf_conntrack_ipv4 iptable_mangle ipt_LOG xt_state ipt_ttl
>>> ipt_MASQUERADE nf_nat nf_conntrack xt_DSCP ip_tables x_tables usbhid
>>> ipw2200 ieee80211 ieee80211_crypt thinkpad_acpi backlight acpi_cpufreq
>>> radeon drm intel_agp agpgart snd_intel8x0 snd_ac97_codec ac97_bus
>>> snd_pcm snd_timer snd soundcore snd_page_alloc button
>>> thermal processor hci_usb bluetooth
```

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btldelconn

```
>>> Feb 7 09:28:06
>>> Feb 7 09:28:06 Pid: 11774, comm: hidd Tainted: G D (2.6.24-git16 #1)
>>> Feb 7 09:28:06 EIP: 0060:[<c0182a99>] EFLAGS: 00010246 CPU: 0
>>> Feb 7 09:28:06 EIP is at sysfs_addrm_start+0x1e/0x7a
>>> Feb 7 09:28:06 EAX: c0394760 EBX: 00000000 ECX: 00000000 EDX: 00000000
>>> Feb 7 09:28:06 ESI: f3733cb4 EDI: f3733cc4 EBP: 00000000 ESP: f3733ca4
>>> Feb 7 09:28:06 DS: 007b ES: 007b FS: 0000 GS: 0033 SS: 0068
>>> Feb 7 09:28:06 Process hidd (pid: 11774, ti=f3732000 task=f3673550
>>> task.ti=f3732000)
>>> Feb 7 09:28:06 Stack: f6c14680 f7f9d6ec ffffffff c0182e80 00000000
>>> 00000000 00000000 00000000
>>> Feb 7 09:28:06 f6c14680 f6c14680 ffffffff f56d563c c0182ee1 f3733cdc
>>> c01c6daa f5fa4c48
>>> Feb 7 09:28:06 c01c6eb9 f6e660f0 00000000 f6c14680 f6e660f0 f56d563c
>>> c01c6fe9 f3733d30
>>> Feb 7 09:28:06 Call Trace:
>>> Feb 7 09:28:06 [<c0182e80>] create_dir+0x33/0x6b
>>> Feb 7 09:28:06 [<c0182ee1>] sysfs_create_dir+0x29/0x3b
>>> Feb 7 09:28:06 [<c01c6daa>] kobject_get+0xf/0x13
>>> Feb 7 09:28:06 [<c01c6eb9>] kobject_add_internal+0xab/0x144
>>> Feb 7 09:28:06 [<c01c6fe9>] kobject_add_varg+0x39/0x42
>>> Feb 7 09:28:06 [<c01c723c>] kobject_add+0x4a/0x4e
>>> Feb 7 09:28:06 [<c0219c62>] get_device_parent+0xd7/0xfb
>>> Feb 7 09:28:06 [<c021a2e1>] device_add+0x79/0x418
>>> Feb 7 09:28:06 [<c01ca789>] snprintf+0x1c/0x1f
>>> Feb 7 09:28:06 [<c026c0e3>] input_register_device+0xb2/0x188
>>> Feb 7 09:28:06 [<c027b9a7>] hidinput_connect+0x24ff/0x2530
>>> Feb 7 09:28:06 [<f895d726>] hidp_send_report+0x143/0x14f [hidp]
>>> Feb 7 09:28:06 [<f895e486>] hidp_sock_ioctl+0xe2/0x1fa [hidp]
>>> Feb 7 09:28:06 [<c0128259>] enqueue_hrtimer+0xd7/0xe2
>>> Feb 7 09:28:06 [<c011375e>] hrtick_set+0x6a/0xc3
>>> Feb 7 09:28:06 [<c0103948>] do_notify_resume+0x5e3/0x644
>>> Feb 7 09:28:06 [<c027f217>] sock_ioctl+0x1ab/0x1cd
>>> Feb 7 09:28:06 [<c027f06c>] sock_ioctl+0x0/0x1cd
>>> Feb 7 09:28:06 [<c015aaa4>] do_ioctl+0x1c/0x5d
>>> Feb 7 09:28:06 [<c015ad11>] vfs_ioctl+0x22c/0x23f
>>> Feb 7 09:28:06 [<c02808b3>] sys_socketcall+0xd2/0x181
>>> Feb 7 09:28:06 [<c015ad50>] sys_ioctl+0x2c/0x44
>>> Feb 7 09:28:06 [<c0103c3a>] sysenter_past_esp+0x5f/0x85
>>> Feb 7 09:28:06 [<c02e0000>] piix_init_one+0x1a7/0x525
>>> Feb 7 09:28:06 =====
>>> Feb 7 09:28:06 Code: 89 f8 e8 3d ff ff ff 31 c0 5b 5e 5f c3 57 b9 04
>>> 00 00 00 56 89 c6 53 31 c0 89 d3 89 f7 f3 ab b8 60 47 39 c0 89 16 e8
>>> 29 f8 15 00 <8b> 53 20 b9 e3 27 18 c0 a1 fc 19 40 c0 53 e8 0c e0 fd ff
>>> 5b 85
>>> Feb 7 09:28:06 EIP: [<c0182a99>] sysfs_addrm_start+0x1e/0x7a SS:ESP
>>> 0068:f3733ca4
>>> Feb 7 09:28:06 ----[ end trace e0c3df2b167f1367 ]----
>>>
>>> # -----
>>>
```

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btdeconn

>>> This does not happen in 2.6.22
>>>
>>> Please let me know if you need more info, or need me to report this elsewhere.
>>
>>
>> Does 2.6.24 work?
>
> Just had an oops w/ 2.6.24.2 and was about to send the attached to
> kml. Although it happens less frequently in 2.6.24.2 and I don't see
> btdeconn in the single Oops I've had in 2.6.24.2
>
>
>> How do you use bluetooth, just as hid devices?
>
> Just one bluetooth mouse.
>
>
>> Could you post full dmesg?
>
> I'll attach the plain text file with most of the output requested by
>
> /usr/src/linux/REPORTING-BUGS
>
> the output of DMESG from after booting to recover from the Oops is at the bottom.
>
>> Regards
>>
>> dave
>
> Thank you!
>
> Barnaby
>

Hi,

Please try the attached patch and help to verify.

Regards
dave

Hi,

Oops is still present, heres what I did..

#bdd 2008-02-15 23:49:09 -----
Added patch...

root@bdianni-lnx:/usr/src# l

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btdeconn

total 52

```
-rw-r--r-- 1 root root 1340 02-15 23:47 diff.txt
lrwxrwxrwx 1 root root 15 02-12 20:58 linux -> linux-2.6.24.2/
```

```
root@bdianni-lnx:/usr/src# patch -p0 < diff.txt
patching file linux/net/bluetooth/hci_conn.c
Hunk #1 succeeded at 265 (offset 5 lines).
patching file linux/net/bluetooth/hci_sysfs.c
Hunk #1 succeeded at 329 (offset -4 lines).
```

#bdd got this during compile..

```
scripts/kconfig/conf -s arch/x86/Kconfig
CHK include/linux/version.h
CHK include/linux/utsrelease.h
CALL scripts/checksyscalls.sh
CHK include/linux/compile.h
GZIP kernel/config_data.gz
IKCFG kernel/config_data.h
CC kernel/configs.o
LD kernel/built-in.o
CC [M] net/bluetooth/hci_conn.o
CC [M] net/bluetooth/hci_sysfs.o
net/bluetooth/hci_sysfs.c: In function 'del_conn':
net/bluetooth/hci_sysfs.c:336: warning: suggest parentheses around
assignment used as truth value
```

#bdd

Rebooted into...

```
root@bdianni-lnx:~# uname -a
Linux bdianni-lnx 2.6.24.2 #8 PREEMPT Fri Feb 15 23:50:59 EST 2008 i686
Intel(R) Pentium(R) M processor 2.13GHz GenuineIntel GNU/Linux
```

```
echo disable > /proc/acpi/ibm/bluetooth
```

results in this oops

```
Feb 16 00:00:49 BUG: unable to handle kernel NULL pointer dereference
at virtual address 00000008
Feb 16 00:00:49 printing eip: c01839b8 *pde = 35841067 *pte = 00000000
Feb 16 00:00:49 Oops: 0000 [#1] PREEMPT
Feb 16 00:00:49 Modules linked in: hidp l2cap vmnet(P) vmmon(P)
snd_seq snd_seq_device snd_pcm_oss snd_mixer_oss ipt_LOG
xt_state nf_conntrack ipt_ttl iptable_filter ip_tables x_tables
sr_mod cdrom usbhid ipw2200 ieee80211 ieee80211_crypt
thinkpad_acpi backlight acpi_cpufreq radeon drm intel_agp
```

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btldelconn

```
agpgart button thermal snd_intel8x0 snd_ac97_codec ac97_bus snd_pcm
snd_timer snd soundcore snd_page_alloc hci_usb 8250_pnp 8250
serial_core bluetooth processor
Feb 16 00:00:49
Feb 16 00:00:49 Pid: 4, comm: events/0 Tainted: P (2.6.24.2 #8)
Feb 16 00:00:49 EIP: 0060:[<c01839b8>] EFLAGS: 00010246 CPU: 0
Feb 16 00:00:49 EIP is at sysfs_move_dir+0x16/0x1d5
Feb 16 00:00:49 EAX: c0393134 EBX: f7de95c0 ECX: f7c45f48 EDX: f7de95c0
Feb 16 00:00:49 ESI: 00000000 EDI: f754e5c0 EBP: ffffffff4 ESP: f7c45f10
Feb 16 00:00:49 DS: 007b ES: 007b FS: 0000 GS: 0000 SS: 0068
Feb 16 00:00:49 Process events/0 (pid: 4, ti=f7c44000 task=f7c3ca90
task. ti=f7c44000)
Feb 16 00:00:49 Stack: ffffffff ffffffff 00000000 c034e4ad f65d56a4
f7de95c0 f754e5c0 f65d56a4
Feb 16 00:00:49 f7de95c0 f754e5c0 ffffffff4 c01c713b f754e2c0 c034e49f
f754e5c0 f754e2c0
Feb 16 00:00:49 f754e2c0 00000000 00000000 f65d563c 00000000 f7de95c0
c021dc05 f65d56a4
Feb 16 00:00:49 Call Trace:
Feb 16 00:00:49 [<c01c713b>] kobject_move+0xa8/0xf3
Feb 16 00:00:49 [<c021dc05>] device_move+0x49/0xd7
Feb 16 00:00:49 [<f886597d>] del_conn+0x18/0x68 [bluetooth]
Feb 16 00:00:49 [<f8865965>] del_conn+0x0/0x68 [bluetooth]
Feb 16 00:00:49 [<c01227bf>] run_workqueue+0x8c/0x128
Feb 16 00:00:49 [<c02ebc9e>] schedule+0x214/0x257
Feb 16 00:00:49 [<c0122db2>] worker_thread+0x0/0xbe
Feb 16 00:00:49 [<c0122e64>] worker_thread+0xb2/0xbe
Feb 16 00:00:49 [<c012562f>] autoremove_wake_function+0x0/0x35
Feb 16 00:00:49 [<c0125575>] kthread+0x36/0x5d
Feb 16 00:00:49 [<c012553f>] kthread+0x0/0x5d
Feb 16 00:00:49 [<c0103ffb>] kernel_thread_helper+0x7/0x10
Feb 16 00:00:49 =====
Feb 16 00:00:49 Code: ff b8 34 31 39 c0 e8 1d 89 16 00 89 f0 83 c4 1c
5b 5e 5f 5d c3 55 57 56 53 89 d3 83 ec 1c 8b 70 1c b8 34 31 39 c0 e8
f3 88 16 00 <8b> 56 08 85 d2 75 04 0f 0b eb fe 8b 5b 1c b8 60 31 39 c0
85 db
Feb 16 00:00:49 EIP: [<c01839b8>] sysfs_move_dir+0x16/0x1d5 SS:ESP
0068: f7c45f10
Feb 16 00:00:49 ---[ end trace 9a444f5bc153934b ]---
```

Thanks,

Barnaby

--

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

Re: 2.6.24-git16 Oops @ sysfs_move_dir w/ btldelconn

6