

2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2003-08/8153.html>

From: Fredrik Noring (noring_at_nocrew.org)

Date: 08/31/03

To: Linux Kernel Development <linux-kernel@vger.kernel.org>

Date: Sun, 31 Aug 2003 00:16:53 +0200

Hi,

Bluetooth performance seems unreliable in 2.6.0-test4 with the Broadcom USB device (a5c/2001). Messages like these appear frequently in the log:

```
drivers/usb/host/uhci-hcd.c: d400: host controller process error.  
something bad happened  
drivers/usb/host/uhci-hcd.c: d400: host controller halted. very bad
```

Sometimes, messages like these also appear:

```
l2cap_recv_acldata: Frame is too short (len 1)  
l2cap_recv_acldata: Unexpected continuation frame (len 124)
```

After a while, the (hci0) interface crashes completely and becomes unusable. The hciconfig tool gives this error:

```
Can't read local name on hci0. Connection timed out(110)
```

Detaching the device from the USB connector gives another crash and a "slab corruption", see call trace below.

Fredrik

```
Aug 30 21:19:53 h9n1fls20o980 kernel: drivers/usb/host/uhci-hcd.c: d400:  
host controller process error. something bad happened  
Aug 30 21:19:53 h9n1fls20o980 kernel: drivers/usb/host/uhci-hcd.c: d400:  
host controller halted. very bad  
Aug 30 21:20:25 h9n1fls20o980 last message repeated 33 times  
Aug 30 21:21:26 h9n1fls20o980 last message repeated 39 times  
Aug 30 21:22:27 h9n1fls20o980 last message repeated 85 times  
Aug 30 21:23:28 h9n1fls20o980 last message repeated 80 times  
Aug 30 21:24:10 h9n1fls20o980 last message repeated 41 times  
Aug 30 21:24:11 h9n1fls20o980 kernel: hci_cmd_task: hci0 command tx  
timeout
```

Linux-Kernel: 2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

```
Aug 30 21:24:11 h9n1fls20o980 kernel: drivers/usb/host/uhci-hcd.c: d400:
host controller halted. very bad
Aug 30 21:24:37 h9n1fls20o980 last message repeated 68 times
Aug 30 21:24:37 h9n1fls20o980 kernel: usb 1-2: USB disconnect, address 4
Aug 30 21:24:37 h9n1fls20o980 kernel: slab error in
cache_free_debugcheck(): cache `size-512': double free, or memory before
object was overwritten
Aug 30 21:24:37 h9n1fls20o980 kernel: Call Trace:
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c013f046>] kfree+0x166/0x360
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e09836d9>]
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e09836d9>]
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e098378d>]
hci_usb_close+0x3d/0x50 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e0984964>]
hci_usb_disconnect+0x24/0x80 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088b168>]
usb_unbind_interface+0x98/0xa0 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0201cd4>]
device_release_driver+0x64/0x70
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0201e49>]
bus_remove_device+0x79/0xc0
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0200d24>] device_del+0x74/0xa0
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0200d63>]
device_unregister+0x13/0x30
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088bcd5>]
usb_disconnect+0xef/0x120 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e378>]
hub_port_connect_change+0x338/0x340 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088d8ea>]
hub_port_status+0x3a/0xb0 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e68a>]
hub_events+0x30a/0x350 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e6fd>] hub_thread+0x2d/0xf0
[usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c010a99e>]
ret_from_fork+0x6/0x14
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0119e60>]
default_wake_function+0x0/0x30
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e6d0>] hub_thread+0x0/0xf0
[usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0108a85>]
kernel_thread_helper+0x5/0x10
Aug 30 21:24:37 h9n1fls20o980 kernel:
Aug 30 21:24:37 h9n1fls20o980 kernel: slab error in
cache_free_debugcheck(): cache `size-512': double free, or memory after
object was overwritten
Aug 30 21:24:37 h9n1fls20o980 kernel: Call Trace:
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c013f072>] kfree+0x192/0x360
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e09836d9>]
```

Linux-Kernel: 2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

```
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e09836d9>]
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e098378d>]
hci_usb_close+0x3d/0x50 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e0984964>]
hci_usb_disconnect+0x24/0x80 [hci_usb]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088b168>]
usb_unbind_interface+0x98/0xa0 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0201cd4>]
device_release_driver+0x64/0x70
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0201e49>]
bus_remove_device+0x79/0xc0
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0200d24>] device_del+0x74/0xa0
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0200d63>]
device_unregister+0x13/0x30
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088bcd5>]
usb_disconnect+0xef/0x120 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e378>]
hub_port_connect_change+0x338/0x340 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088d8ea>]
hub_port_status+0x3a/0xb0 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e68a>]
hub_events+0x30a/0x350 [usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e6fd>] hub_thread+0x2d/0xf0
[usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c010a99e>]
ret_from_fork+0x6/0x14
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0119e60>]
default_wake_function+0x0/0x30
Aug 30 21:24:37 h9n1fls20o980 kernel: [<e088e6d0>] hub_thread+0x0/0xf0
[usbcore]
Aug 30 21:24:37 h9n1fls20o980 kernel: [<c0108a85>]
kernel_thread_helper+0x5/0x10
Aug 30 21:24:37 h9n1fls20o980 kernel:
Aug 30 21:24:37 h9n1fls20o980 kernel: -----[ cut here
]-----
Aug 30 21:24:37 h9n1fls20o980 kernel: kernel BUG at mm/slab.c:1659!
Aug 30 21:24:37 h9n1fls20o980 kernel: invalid operand: 0000 [#1]
Aug 30 21:24:37 h9n1fls20o980 kernel: CPU: 0
Aug 30 21:24:37 h9n1fls20o980 kernel: EIP: 0060:[<c013f17d>] Not
tainted
Aug 30 21:24:37 h9n1fls20o980 kernel: EFLAGS: 00010016
Aug 30 21:24:37 h9n1fls20o980 kernel: EIP is at kfree+0x29d/0x360
Aug 30 21:24:37 h9n1fls20o980 kernel: eax: d3e7c28c ebx: 00010c00
ecx: 0000020c edx: 00000009
Aug 30 21:24:37 h9n1fls20o980 kernel: esi: dffffb580 edi: d3e7c080
ebp: d3e7c295 esp: dec29e50
Aug 30 21:24:37 h9n1fls20o980 kernel: ds: 007b es: 007b ss: 0068
Aug 30 21:24:37 h9n1fls20o980 kernel: Process khubd (pid: 78,
threadinfo=dec28000 task=dec6ec80)
```

Linux-Kernel: 2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

```
Aug 30 21:24:37 h9n1fls20o980 kernel: Stack: c02bd20d dffffb580 c02cd6e0
db903afc 00000208 e09836d9 dfff6190 00000286
Aug 30 21:24:38 h9n1fls20o980 kernel: db62f4d8 db62f4ec d485f4e4
d485f4c4 e09836d9 d3e7c299 d485f4e4 00000000
Aug 30 21:24:38 h9n1fls20o980 kernel: d485f310 e0985e9c c17967d8
e0985e20 e098378d d485f310 d485f310 e0984964
Aug 30 21:24:38 h9n1fls20o980 kernel: Call Trace:
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e09836d9>]
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e09836d9>]
hci_usb_unlink_urbs+0x99/0x110 [hci_usb]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e098378d>]
hci_usb_close+0x3d/0x50 [hci_usb]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e0984964>]
hci_usb_disconnect+0x24/0x80 [hci_usb]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088b168>]
usb_unbind_interface+0x98/0xa0 [usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0201cd4>]
device_release_driver+0x64/0x70
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0201e49>]
bus_remove_device+0x79/0xc0
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0200d24>] device_del+0x74/0xa0
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0200d63>]
device_unregister+0x13/0x30
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088bcd5>]
usb_disconnect+0xef/0x120 [usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088e378>]
hub_port_connect_change+0x338/0x340 [usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088d8ea>]
hub_port_status+0x3a/0xb0 [usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088e68a>]
hub_events+0x30a/0x350 [usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088e6fd>] hub_thread+0x2d/0xf0
[usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c010a99e>]
ret_from_fork+0x6/0x14
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0119e60>]
default_wake_function+0x0/0x30
Aug 30 21:24:38 h9n1fls20o980 kernel: [<e088e6d0>] hub_thread+0x0/0xf0
[usbcore]
Aug 30 21:24:38 h9n1fls20o980 kernel: [<c0108a85>]
kernel_thread_helper+0x5/0x10
Aug 30 21:24:38 h9n1fls20o980 kernel:
Aug 30 21:24:38 h9n1fls20o980 kernel: Code: 0f 0b 7b 06 13 cb 2c c0 e9
26 ff ff ff 0f 0b 7a 06 13 cb 2c
Aug 30 21:24:38 h9n1fls20o980 kernel: <3>drivers/usb/host/uhci-hcd.c:
d400: host controller halted. very bad
Aug 30 21:24:38 h9n1fls20o980 kernel: drivers/usb/host/uhci-hcd.c: d400:
host controller halted. very bad
Aug 30 21:24:38 h9n1fls20o980 kernel: drivers/usb/host/uhci-hcd.c: d400:
host controller halted. very bad
```

Linux-Kernel: 2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

Aug 30 21:25:14 h9n1fls20o980 kernel: hci_cmd_task: hci0 command tx timeout

Aug 30 21:25:32 h9n1fls20o980 hcid[1025]: HCI dev 0 down

Aug 30 21:25:32 h9n1fls20o980 hcid[1025]: Stopping security manager 0

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Hangup (SIGHUP)

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Modem hangup

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Connection terminated.

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Connect time 9.7 minutes.

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Sent 129231 bytes, received 904184 bytes.

Aug 30 21:25:32 h9n1fls20o980 /etc/hotplug/net.agent: NET remove event not supported

Aug 30 21:25:32 h9n1fls20o980 pppd[3458]: Exit.

Aug 30 21:25:36 h9n1fls20o980 kernel: hci_usb_intr_rx_submit: hci0 intr rx submit failed urb cf7b2d20 err -19

Aug 30 21:28:36 h9n1fls20o980 kernel: uhci-hcd 0000:00:09.0: remove, state 3

Aug 30 21:28:36 h9n1fls20o980 kernel: usb usb1: USB disconnect, address 1

Aug 30 21:56:57 h9n1fls20o980 kernel: Slab corruption: start=d3e7c49c, expend=d3e7c69b, problemat=d3e7c49d

Aug 30 21:56:57 h9n1fls20o980 kernel: Last user:

[<c0250ae3>](kfree_skbmem+0x13/0x30)

Aug 30 21:56:57 h9n1fls20o980 kernel: Data: .D9 36 98 E0

Aug 30 21:56:57 h9n1fls20o980 kernel: Next: 71 F0 2C .E3 0A 25 C0 A5 C2 0F 17 80 01 06 00 00 00 00 00 BC 00 A0 00 00 00 00 00 00 00 00

Aug 30 21:56:57 h9n1fls20o980 kernel: slab error in check_poison_obj():

cache `size-512': object was modified after freeing

Aug 30 21:56:57 h9n1fls20o980 kernel: Call Trace:

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c013d398>]

check_poison_obj+0x168/0x1b0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c013eba8>]

__kmallocc+0x168/0x1d0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02508e7>] alloc_skb+0x47/0xe0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02508e7>] alloc_skb+0x47/0xe0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0250103>]

sock_alloc_send_skb+0xc3/0x1d0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c025023f>]

sock_alloc_send_skb+0x2f/0x40

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02ae232>]

unix_stream_sendmsg+0x192/0x3b0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c01a4a56>]

avc_has_perm+0x76/0x8c

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c024d18f>]

sock_aio_write+0xef/0x100

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153b2b>]

do_sync_write+0x8b/0xc0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c01a58b9>]

inode_has_perm+0x69/0xa0

Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153c7d>]

Linux-Kernel: 2.6.0-test4: uhci-hcd.c: "host controller process error", slab call trace

```
vfs_write+0x11d/0x150
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153d62>] sys_write+0x42/0x70
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c010aa39>]
sysenter_past_esp+0x52/0x71
Aug 30 21:56:57 h9n1fls20o980 kernel:
Aug 30 21:56:57 h9n1fls20o980 kernel: slab error in
cache_alloc_debugcheck_after(): cache `size-512': memory before object
was overwritten
Aug 30 21:56:57 h9n1fls20o980 kernel: Call Trace:
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c013eb38>] __kmalloc+0xf8/0x1d0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02508e7>] alloc_skb+0x47/0xe0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02508e7>] alloc_skb+0x47/0xe0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0250103>]
sock_alloc_send_skb+0xc3/0x1d0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c025023f>]
sock_alloc_send_skb+0x2f/0x40
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c02ae232>]
unix_stream_sendmsg+0x192/0x3b0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c01a4a56>]
avc_has_perm+0x76/0x8c
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c024d18f>]
sock_aio_write+0xef/0x100
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153b2b>]
do_sync_write+0x8b/0xc0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c01a58b9>]
inode_has_perm+0x69/0xa0
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153c7d>]
vfs_write+0x11d/0x150
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c0153d62>] sys_write+0x42/0x70
Aug 30 21:56:57 h9n1fls20o980 kernel: [<c010aa39>]
sysenter_past_esp+0x52/0x71
Aug 30 21:56:57 h9n1fls20o980 kernel:
Aug 30 21:58:29 h9n1fls20o980 shutdown: shutting down for system reboot
```

-

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/>