

Re: [linux-usb-devel] Re: [OOPS, usbcore, releaseintf] 2.6.0-test10-mm1

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2003-12/2098.html>

From: Alan Stern (*stern_at_rowland.harvard.edu*)

Date: 12/09/03

Date: Tue, 9 Dec 2003 10:47:42 -0500 (EST)

To: Duncan Sands <baldrick@free.fr>

On Tue, 9 Dec 2003, Duncan Sands wrote:

> *Maybe this is related to "oopses in kobjects in 2.6.0-test11 (was Re: kobject patch)"?*
> *My call to usb_put_dev in usbdev_release is releasing the kobject,*
> *which shows that the reference count was not already zero. However*
> *it dereferences a NULL pointer in here:*
>
> *static void hcd_pci_release(struct usb_bus *bus)*
> *{*
> *struct usb_hcd *hcd = bus->hcpriv;*
>
> *if(hcd)*
> *hcd->driver->hcd_free(hcd);*
> *}*
>
> *which suggests that the hcd was already released. Maybe Greg can comment?*
>
> *[9889]: shutting down for system reboot*
> *printing eip:*
> *c8ae8999*
> *Oops: 0000 [#1]*
> *PREEMPT*
> *CPU: 0*
> *EIP: 0060:[<c8ae8999>] Not tainted VLI*
> *EFLAGS: 00010286*
> *EIP is at hcd_pci_release+0x19/0x20 [usbcore]*
> *eax: c8c69d80 ebx: c637f050 ecx: c8af6c20 edx: c637f000*
> *esi: c031e65c edi: c031e680 ebp: c0019ec4 esp: c0019ec0*
> *ds: 007b es: 007b ss: 0068*
> *Process modem_run (pid: 8460, threadinfo=c0018000 task=c1508080)*
> *Stack: c637f000 c0019ed0 c8ae455d c637f000 c0019ee8 c0203738 c637f048*
> *c0019f00*
> *c8ae77d6 c031e450 c0019f00 c01bc88f c637f050 c6b09200 c031e428 c031e440*
> *c0019f10 c8ae08b6 c637f050 00000000 c0019f2c c02019e1 c6b092cc c0019f2c*
> *Call Trace:*

```
> [c8ae455d>] usb_host_release+0x1d/0x20 [usbcore]
> [c0203738>] class_dev_release+0x58/0x60
> [c8ae77d6>] usb_destroy_configuration+0xb6/0xf0 [usbcore]
> [c01bc88f>] kobject_cleanup+0x6f/0x80
> [c8ae08b6>] usb_release_dev+0x46/0x60 [usbcore]
> [c02019e1>] device_release+0x21/0x80
> [c01bc88f>] kobject_cleanup+0x6f/0x80
> [c8ae9b38>] usbdev_release+0x88/0xc0 [usbcore]
> [c0157a5c>] __fput+0x10c/0x120
> [c0156047>] filp_close+0x57/0x80
> [c01560d1>] sys_close+0x61/0x90
> [c02a302e>] sysenter_past_esp+0x43/0x65
>
> Code: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 55 89 e5 83
> ec 04 8b 45 08 8b 50 30 85 d2 74 0c 8b 82 08 01 00 00 89 14 24 <ff> 50
> 28 c9 c3 89 f6 55 89 e5 57 56 53 83 ec 34 8b 5d 0c e8 3f
```

I don't understand this stack dump. The EIP address is `_after the end_` of `hcd_pci_release`, as you can see from the fact that the following code is nothing but a long string of NOPS. Also, I don't understand the cause of the oops. What does the PREEMPT mean? There's no indication that a null pointer was dereferenced. None of the registers contains 0.

But if you think that's the problem, try adding a `printk` to `hcd_pci_release` to display the values of `bus`, `hcd->driver`, and `hcd->driver->hcd_free`. Knowing which one is NULL ought to help your analysis.

Alan Stern

-

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/>