

Re: 2.6.0-test9-mm4 (does not boot)

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2003-12/0470.html>

From: Adam Belay (ambx1_at_neo.rr.com)

Date: 12/02/03

Date: Tue, 2 Dec 2003 22:28:44 +0000
To: Frank Dekervel <kervel@drie.kotnet.org>

On Mon, Nov 24, 2003 at 09:10:29AM +0100, Frank Dekervel wrote:

> *Op Monday 24 November 2003 00:05, schreef u:*
> > > *– will the original behaviour really solve the problem ?(not only a*
> > > *symptom) ? as i wrote, i can trigger almost the same oops (general*
> > > *protection fault #0000 , invalid EIP value), probably non-fatal because*
> > > *another process is killed instead of the pid=1 process, and i can trigger*
> > > *it on a mm4 with all pnpbios fixes backed out ...*

Is the oops triggered by reading /proc/bus/pnp/devices a general protection fault?
Once in a while it will produce a different error in userspace. If so, I'd like
to see the output.

> >
> > *Yes but through the /proc/bus/pnp/devices file. ?Correct? ?It is*
> > *independent from this change and would also need to be corrected. ?Does the*
> > *escd interface in /proc/bus/pnp also trigger an oops?*
>
> *yup it seems so, but this time with valid backtrace*
> *bakvis:/proc/bus/pnp# cat escd*
> *Segmentation fault*

Could you please try this patch (without pnp-patch-1)... It may fix the ESCD
reading problem. If it doesn't oops when catted, you may want to test it out
with lsescd by Gunther Mayer.

(<http://home.t-online.de/home/gunther.mayer/lsecd-0.10.tar.bz2>)

```
--- a/drivers/pnp/pnpbios/bioscalls.c 2003-11-26 20:44:47.000000000 +0000
+++ b/drivers/pnp/pnpbios/bioscalls.c 2003-12-02 21:17:42.000000000 +0000
@@ -493,7 +493,7 @@
     if (!pnp_bios_present())
         return ESCD_FUNCTION_NOT_SUPPORTED;
     status = call_pnp_bios(PNP_READ_ESCD, 0, PNP_TS1, PNP_TS2, PNP_DS, 0, 0, 0,
- data, 65536, (void *)nvrnram_base, 65536);
+ data, 65536, __va((void *)nvrnram_base), 65536);
     return status;
 }
```

Linux-Kernel: Re: 2.6.0-test9-mm4 (does not boot)

```
@@ -516,7 +516,7 @@
    if (!pnp_bios_present())
        return ESCD_FUNCTION_NOT_SUPPORTED;
    status = call_pnp_bios(PNP_WRITE_ESCD, 0, PNP_TS1, PNP_TS2, PNP_DS, 0, 0, 0,
- data, 65536, nvram_base, 65536);
+ data, 65536, __va((void *)nvram_base), 65536);
    return status;
}
#endif
```

Also just out of curiosity, could I see what the real mode CS and DS are? I'm looking for patterns...

So far all of the offenders have a datasegment at 0xf0000.

```
--- a/drivers/pnp/pnpbios/core.c 2003-11-26 20:42:52.000000000 +0000
+++ b/drivers/pnp/pnpbios/core.c 2003-12-02 21:59:18.000000000 +0000
@@ -460,6 +460,9 @@
    check->fields.version >> 4, check->fields.version & 15,
    check->fields.pm16cseg, check->fields.pm16offset,
    check->fields.pm16dseg);
+ printk(KERN_INFO "PnPBIOS: realmode entry 0x%x:0x%x, dseg 0x%x\n",
+ check->fields.rmcseg, check->fields.rmoffset,
+ check->fields.rmdseg);
    pnp_bios_install = check;
    return 1;
}
```

Thanks,
Adam

-

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/>

Re: 2.6.0-test9-mm4 (does not boot)