Subject: Re: [PATCH] Fix OOPS in show_uevent()
Posted by Kay Sievers on Fri, 10 Aug 2007 12:23:56 GMT
View Forum Message <> Reply to Message

On 8/10/07, Pavel Emelyanov <xemul@openvz.org> wrote:
> The platform_uevent() callback called via
> show_uevent()
> dev_uevent()
> platform_uevent()
> forgot to set NULL to the last envp pointer and this caused the
> show_uevent() oops while printing all the envp pointers like this:

> The last hunk in this patch fixes this.

Looks like the right fix, yes.

> The other problem is that the envp passed to bus, type and platform callbacks
> from dev_uevent() is the same, so the callbacks can overwrite the info, written
> by the others. Did I miss something important?

Sounds like a bug, yes.

But we still don't update the remaining buffer size and the remaining
array fields which are left after the call. Shouldn't we instead just
change the:
```
  int (*dev_uevent)(struct device *dev,
                    char **envp, int num_envp,
                    char *buffer, int buffer_size);
```
to:
```
 int (*dev_uevent)(struct device *dev,
                   char **envp, int num_envp, int *cur_index,
                   char *buffer, int buffer_size, int *cur_len);
```

like we do for:
```
 int add_uevent_var(char **envp, int num_envp, int *cur_index,
                    char *buffer, int buffer_size, int *cur_len,
                    const char *format, ...)
```

and along with the change of the callers, we would update the values
properly, so the next call has the correct numbers? There are 6
classes and something like 12 buses using this method, so it shouldn't
be too much trouble.

Thanks,
Kay