[PATCH] usb: storage: add error handling for kcalloc

9 messages

Zhouyang Jia <jiazhouyang09@gmail.com> Mon, Jun 11, 2018 at 4:52 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, Alan Stern <stern@rowland.harvard.edu>, Greg Kroah-Hartman <gregkh@linuxfoundation.org>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

When kcalloc fails, the lack of error-handling code may
cause unexpected results.

This patch adds error-handling code after calling kcalloc.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
---
drivers/usb/storage/alauda.c | 5 +++++
1 file changed, 5 insertions(+)

```
diff --git a/drivers/usb/storage/alauda.c b/drivers/usb/storage/alauda.c
index 900591d..c56355c 100644
--- a/drivers/usb/storage/alauda.c
+++ b/drivers/usb/storage/alauda.c
@@ -437,6 +437,11 @@ static int alauda_init_media(struct us_data *us)
                + MEDIA_INFO(us).blockshift + MEDIA_INFO(us).pageshift);
        MEDIA_INFO(us).pba_to_lba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
        MEDIA_INFO(us).lba_to_pba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
+       if ((MEDIA_INFO(us).pba_to_lba == NULL)
+               || (MEDIA_INFO(us).lba_to_pba == NULL)) {
+               pr_warn("alauda_init_media: memory allocation failed\n");
+               return USB_STOR_TRANSPORT_ERROR;
+       }

        if (alauda_reset_media(us) != USB_STOR_XFER_GOOD)
                return USB_STOR_TRANSPORT_ERROR;
--
2.7.4
```

Greg Kroah-Hartman <gregkh@linuxfoundation.org> Mon, Jun 11, 2018 at 4:27 PM
To: Zhouyang Jia <jiazhouyang09@gmail.com>

[Quoted text hidden]

> --
> To unsubscribe from this list: send the line "unsubscribe linux-usb" in
> the body of a message to majordomo@vger.kernel.org
> More majordomo info at http://vger.kernel.org/majordomo-info.html

Hi,

This is the friendly semi-automated patch-bot of Greg Kroah-Hartman.
You have sent him a patch that has triggered this response.

Right now, the development tree you have sent a patch for is "closed"
due to the timing of the merge window. Don't worry, the patch(es) you
have sent are not lost, and will be looked at after the merge window is
over (after the -rc1 kernel is released by Linus).

So thank you for your patience and your patches will be reviewed at this
later time, you do not have to do anything further, this is just a short
note to let you know the patch status and so you don't worry they didn't
make it through.

thanks,

greg k-h's patch email bot

Alan Stern <stern@rowland.harvard.edu> Tue, Jun 12, 2018 at 10:31 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Greg Kroah-Hartman <gregkh@linuxfoundation.org>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

On Mon, 11 Jun 2018, Zhouyang Jia wrote:

> When kcalloc fails, the lack of error-handling code may
> cause unexpected results.
>
> This patch adds error-handling code after calling kcalloc.
>
> Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> ---
> drivers/usb/storage/alauda.c | 5 +++++
> 1 file changed, 5 insertions(+)
>
> diff --git a/drivers/usb/storage/alauda.c b/drivers/usb/storage/alauda.c
> index 900591d..c56355c 100644
> --- a/drivers/usb/storage/alauda.c
> +++ b/drivers/usb/storage/alauda.c
> @@ -437,6 +437,11 @@ static int alauda_init_media(struct us_data *us)
>   + MEDIA_INFO(us).blockshift + MEDIA_INFO(us).pageshift);
>   MEDIA_INFO(us).pba_to_lba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
>   MEDIA_INFO(us).lba_to_pba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
> +   if ((MEDIA_INFO(us).pba_to_lba == NULL)
> + || (MEDIA_INFO(us).lba_to_pba == NULL)) {
> +   pr_warn("alauda_init_media: memory allocation failed\n");
> +   return USB_STOR_TRANSPORT_ERROR;
> +   }

pr_info() isn't a good routine to use here, because it doesn't print
the device or driver name.

In any case, a log message isn't necessary. kcalloc() will already
put a message in the log if either of the allocations fails.

Alan Stern
[Quoted text hidden]

Zhouyang Jia <jiazhouyang09@gmail.com> Thu, Jun 14, 2018 at 12:45 AM
To: Alan Stern <stern@rowland.harvard.edu>
Cc: Greg Kroah-Hartman <gregkh@linuxfoundation.org>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

Hi,

Thanks for your kind reply.

Should we still need to handle the error? I mean returning directly
instead of printing a message.

I'll remove the pr_warn statement in v2 if necessary.

Best,
Zhouyang
[Quoted text hidden]

Zhouyang Jia <jiazhouyang09@gmail.com> Thu, Jun 14, 2018 at 9:29 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, Alan Stern <stern@rowland.harvard.edu>, Greg Kroah-Hartman <gregkh@linuxfoundation.org>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

When kcalloc fails, the lack of error-handling code may
cause unexpected results.

This patch adds error-handling code after calling kcalloc.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
---
v1->v2:
- Remove pr_warn statement.
---
drivers/usb/storage/alauda.c | 3 +++
1 file changed, 3 insertions(+)

```
diff --git a/drivers/usb/storage/alauda.c b/drivers/usb/storage/alauda.c
index 900591d..4e17609 100644
--- a/drivers/usb/storage/alauda.c
+++ b/drivers/usb/storage/alauda.c
@@ -437,6 +437,9 @@ static int alauda_init_media(struct us_data *us)
                + MEDIA_INFO(us).blockshift + MEDIA_INFO(us).pageshift);
        MEDIA_INFO(us).pba_to_lba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
        MEDIA_INFO(us).lba_to_pba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
+       if ((MEDIA_INFO(us).pba_to_lba == NULL)
+               || (MEDIA_INFO(us).lba_to_pba == NULL))
+               return USB_STOR_TRANSPORT_ERROR;
```

[Quoted text hidden]

Alan Stern <stern@rowland.harvard.edu> Thu, Jun 14, 2018 at 10:58 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Greg Kroah-Hartman <gregkh@linuxfoundation.org>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

On Thu, 14 Jun 2018, Zhouyang Jia wrote:

> When kcalloc fails, the lack of error-handling code may
> cause unexpected results.
>
> This patch adds error-handling code after calling kcalloc.
>
> Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> ---
> v1->v2:
> - Remove pr_warn statement.
> ---
> drivers/usb/storage/alauda.c | 3 +++
> 1 file changed, 3 insertions(+)
>
> diff --git a/drivers/usb/storage/alauda.c b/drivers/usb/storage/alauda.c
> index 900591d..4e17609 100644
> --- a/drivers/usb/storage/alauda.c
> +++ b/drivers/usb/storage/alauda.c
> @@ -437,6 +437,9 @@ static int alauda_init_media(struct us_data *us)
> 			+ MEDIA_INFO(us).blockshift + MEDIA_INFO(us).pageshift);
> 	MEDIA_INFO(us).pba_to_lba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
> 	MEDIA_INFO(us).lba_to_pba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
> +	if ((MEDIA_INFO(us).pba_to_lba == NULL)
> +	 || (MEDIA_INFO(us).lba_to_pba == NULL))
> +		return USB_STOR_TRANSPORT_ERROR;
>
> 	if (alauda_reset_media(us) != USB_STOR_XFER_GOOD)
> 		return USB_STOR_TRANSPORT_ERROR;
>

Acked-by: Alan Stern <stern@rowland.harvard.edu>

Greg Kroah-Hartman <gregkh@linuxfoundation.org> Mon, Jun 25, 2018 at 8:33 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Alan Stern <stern@rowland.harvard.edu>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

On Thu, Jun 14, 2018 at 09:29:11PM +0800, Zhouyang Jia wrote:
> When kcalloc fails, the lack of error-handling code may
> cause unexpected results.
>
> This patch adds error-handling code after calling kcalloc.
>
> Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> Acked-by: Alan Stern <stern@rowland.harvard.edu>
> ---
> v1->v2:
> - Remove pr_warn statement.
> ---
> drivers/usb/storage/alauda.c | 3 +++
> 1 file changed, 3 insertions(+)
>
> diff --git a/drivers/usb/storage/alauda.c b/drivers/usb/storage/alauda.c
> index 900591d..4e17609 100644
> --- a/drivers/usb/storage/alauda.c
> +++ b/drivers/usb/storage/alauda.c
> @@ -437,6 +437,9 @@ static int alauda_init_media(struct us_data *us)
> 			+ MEDIA_INFO(us).blockshift + MEDIA_INFO(us).pageshift);
> 	MEDIA_INFO(us).pba_to_lba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
> 	MEDIA_INFO(us).lba_to_pba = kcalloc(num_zones, sizeof(u16*), GFP_NOIO);
> +	if ((MEDIA_INFO(us).pba_to_lba == NULL)
> +	 || (MEDIA_INFO(us).lba_to_pba == NULL))
> +		return USB_STOR_TRANSPORT_ERROR;

You just leaked memory if only one of these succeeded :(

Alan Stern <stern@rowland.harvard.edu> Mon, Jun 25, 2018 at 11:22 AM
To: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

[Quoted text hidden]
That's not really true. The memory gets deallocated later on in any
case, when alauda_info_destructor() calls alauda_free_maps() if not
before.

More troubling is the fact that this routine (i.e, alauda_init_media)
gets called from only one place, in alauda_check_media, and the caller
completely ignores the return value! Furthermore, the caller always
returns USB_STOR_TRANSPORT_FAILED.

So on the whole, I don't think this patch is going to make any
difference to the driver's operation.

Alan Stern

Greg Kroah-Hartman <gregkh@linuxfoundation.org> Thu, Jun 28, 2018 at 6:52 AM
To: Alan Stern <stern@rowland.harvard.edu>
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, linux-usb@vger.kernel.org, usb-storage@lists.one-eyed-alien.net, linux-kernel@vger.kernel.org

[Quoted text hidden]
Ok, I'm just going to drop it then.

thanks,

greg k-h