[PATCH] target: add error handling for match_int

3 messages

Zhouyang Jia <jiazhouyang09@gmail.com> Tue, Jun 12, 2018 at 12:52 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, "Nicholas A. Bellinger" <nab@linux-iscsi.org>, linux-scsi@vger.kernel.org, target-devel@vger.kernel.org, linux-kernel@vger.kernel.org

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

This patch adds error-handling code after calling match_int.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
---
drivers/target/target_core_rd.c | 6 ++++--
1 file changed, 4 insertions(+), 2 deletions(-)

```
diff --git a/drivers/target/target_core_rd.c b/drivers/target/target_core_rd.c
index a6e8106..7bc89ff 100644
--- a/drivers/target/target_core_rd.c
+++ b/drivers/target/target_core_rd.c
@@ -573,14 +573,16 @@ static ssize_t rd_set_configfs_dev_params(struct se_device *dev,
                token = match_token(ptr, tokens, args);
                switch (token) {
                case Opt_rd_pages:
-                       match_int(args, &arg);
+                       if (match_int(args, &arg))
+                               return -EINVAL;
                        rd_dev->rd_page_count = arg;
                        pr_debug("RAMDISK: Referencing Page"
                                " Count: %u\n", rd_dev->rd_page_count);
                        rd_dev->rd_flags |= RDF_HAS_PAGE_COUNT;
                        break;
                case Opt_rd_nullio:
-                       match_int(args, &arg);
+                       if (match_int(args, &arg))
+                               return -EINVAL;
                        if (arg != 1)
                                break;
```

--
2.7.4

Bart Van Assche <Bart.VanAssche@wdc.com> Tue, Jun 12, 2018 at 9:25 AM
To: "jiazhouyang09@gmail.com" <jiazhouyang09@gmail.com>
Cc: "linux-scsi@vger.kernel.org" <linux-scsi@vger.kernel.org>, "linux-kernel@vger.kernel.org" <linux-kernel@vger.kernel.org>, "target-devel@vger.kernel.org" <target-devel@vger.kernel.org>, "nab@linux-iscsi.org" <nab@linux-iscsi.org>

[Quoted text hidden]
Please return the error code returned by match_int() instead of -EINVAL.

Thanks,

Bart.

James Bottomley <James.Bottomley@hansenpartnership.com> Tue, Jun 12, 2018 at 5:21 PM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: "Nicholas A. Bellinger" <nab@linux-iscsi.org>, linux-scsi@vger.kernel.org, target-devel@vger.kernel.org, linux-kernel@vger.kernel.org

On Tue, 2018-06-12 at 12:52 +0800, Zhouyang Jia wrote:
> When match_int fails, the lack of error-handling code may
> cause unexpected results.
>
> This patch adds error-handling code after calling match_int.
>
> Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> ---
> drivers/target/target_core_rd.c | 6 ++++--
> 1 file changed, 4 insertions(+), 2 deletions(-)
>
> diff --git a/drivers/target/target_core_rd.c
> b/drivers/target/target_core_rd.c
> index a6e8106..7bc89ff 100644
> --- a/drivers/target/target_core_rd.c
> +++ b/drivers/target/target_core_rd.c
> @@ -573,14 +573,16 @@ static ssize_t
> rd_set_configfs_dev_params(struct se_device *dev,
>   token = match_token(ptr, tokens, args);
>   switch (token) {
>   case Opt_rd_pages:
> -   match_int(args, &arg);
> +   if (match_int(args, &arg))
> +   return -EINVAL;

The first observation is that this would leak the kmalloc'd orig
variable, but the second is that I don't think terminating parsing is
the right thing to do even if match_int() returns an error: just
ignoring this option and proceed to the next seems to be the best
course because that's what we do with unrecognised options (the
default: case).

James