author	Yu Kuai <yukuai3@huawei.com>	2023-03-15 14:21:54 +0800
committer	Martin K. Petersen <martin.petersen@oracle.com>	2023-03-16 23:02:23 -0400
commit	a13faca032acbf2699293587085293bdfaafc8ae (patch)	
tree	fa64699789d2598d8773d8a31155fc8c60fe7981	
parent	d3affdeb400f3adc925bd996f3839481f5291839 (diff)	
download	linux-a13faca032acbf2699293587085293bdfaafc8ae.tar.gz	

scsi: scsi_dh_alua: Fix memleak for 'qdata' in alua_activate()

```
If alua_rtpg_queue() failed from alua_activate(), then 'qdata' is not
freed, which will cause following memleak:

unreferenced object 0xffff88810b2c6980 (size 32):
  comm "kworker/u16:2", pid 635322, jiffies 4355801099 (age 1216426.076s)
  hex dump (first 32 bytes):
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    40 39 24 c1 ff ff ff ff 00 f8 ea 0a 81 88 ff ff  @9$.............
  backtrace:
    [<0000000098f3a26d>] alua_activate+0xb0/0x320
    [<000000003b529641>] scsi_dh_activate+0xb2/0x140
    [<000000007b296db3>] activate_path_work+0xc6/0xe0 [dm_multipath]
    [<000000007adc9ace>] process_one_work+0x3c5/0x730
    [<00000000c457a985>] worker_thread+0x93/0x650
    [<00000000cb80e628>] kthread+0x1ba/0x210
    [<00000000a1e61077>] ret_from_fork+0x22/0x30

Fix the problem by freeing 'qdata' in error path.

Fixes: 625fe857e4fa ("scsi: scsi_dh_alua: Check scsi_device_get() return value")
Signed-off-by: Yu Kuai <yukuai3@huawei.com>
Link: https://lore.kernel.org/r/20230315062154.668812-1-yukuai1@huaweicloud.com
Reviewed-by: Benjamin Block <bblock@linux.ibm.com>
Reviewed-by: Bart Van Assche <bvanassche@acm.org>
Signed-off-by: Martin K. Petersen <martin.petersen@oracle.com>
```

Diffstat

-rw-r--r-- drivers/scsi/device_handler/scsi_dh_alua.c 6

1 files changed, 4 insertions, 2 deletions

```
diff --git a/drivers/scsi/device_handler/scsi_dh_alua.c b/drivers/scsi/device_handler/scsi_dh_alua.c
index 362fa631f39b26..a226dc1b65d715 100644
--- a/drivers/scsi/device_handler/scsi_dh_alua.c
+++ b/drivers/scsi/device_handler/scsi_dh_alua.c
@@ -1145,10 +1145,12 @@ static int alua_activate(struct scsi_device *sdev,
        rcu_read_unlock();
        mutex_unlock(&h->init_mutex);

-       if (alua_rtpg_queue(pg, sdev, qdata, true))
+       if (alua_rtpg_queue(pg, sdev, qdata, true)) {
                fn = NULL;
-       else
+       } else {
```

```
+                kfree(qdata);
                 err = SCSI_DH_DEV_OFFLINED;
+        }
         kref_put(&pg->kref, release_port_group);
 out:
         if (fn)
```