



index : kernel/git/stable/linux.git

Linux kernel stable tree

master

switch

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg

search

author Yu Kuai <yukuai3@huawei.com> 2023-03-15 14:21:54 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-30 12:49:03 +0200
commit [1c55982beb80c7d3c30278fc6cfd8496a31dbe6](#) (patch)
tree [56070dbb154385cf4f2f775723ef85c9d65774b1](#)
parent [a0de3f29d8785b67a1502702ba8fd6e938f8ed5c](#) (diff)
download [linux-1c55982beb80c7d3c30278fc6cfd8496a31dbe6.tar.gz](#)

diff options

context:
space:
mode:

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

[Upstream commit [a13faca032acbf2699293587085293bdfaafc8ae](#)]

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
    [<0000000003b529641>] scsi_dh_activate+0xb2/0x140
    [<0000000007b296db3>] activate_path_work+0xc6/0xe0 [dm_multipath]
    [<0000000007adc9ace>] process_one_work+0x3c5/0x730
    [<000000000c457a985>] worker_thread+0x93/0x650
    [<000000000cb80e628>] kthread+0x1ba/0x210
    [<000000000a1e61077>] 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>
Signed-off-by: Sasha Levin <sashal@kernel.org>

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 610a51538f0347..0781f991e78456 100644

--- a/drivers/scsi/device_handler/scsi_dh_alua.c

+++ b/drivers/scsi/device_handler/scsi_dh_alua.c

```
@@ -1117,10 +1117,12 @@ 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)
```