



author Justin Tee <justin.tee@broadcom.com> 2023-02-27 20:43:36 -0800
committer Martin K. Petersen <martin.petersen@oracle.com> 2023-03-06 18:33:12 -0500
commit [312320b0e0ec21249a17645683fe5304d796aec1](#) (patch)
tree [dbe7bbe2863dfd69c539fdf767550e45ef54f80c](#)
parent [c9507eab9fa7af7ab4c80856eeafd1481ff16f7c](#) (diff)
download [linux-312320b0e0ec21249a17645683fe5304d796aec1.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

scsi: lpfc: Check kzalloc() in lpfc_sli4_cgn_params_read()

If kzalloc() fails in lpfc_sli4_cgn_params_read(), then we rely on lpfc_read_object()'s routine to NULL check pdata.

Currently, an early return error is thrown from lpfc_read_object() to protect us from NULL ptr dereference, but the errno code is -ENODEV.

Change the errno code to a more appropriate -ENOMEM.

Reported-by: Kang Chen <void0red@gmail.com>

Link: <https://lore.kernel.org/all/20230226102338.3362585-1-void0red@gmail.com>

Signed-off-by: Justin Tee <justin.tee@broadcom.com>

Link: <https://lore.kernel.org/r/20230228044336.5195-1-justintee8345@gmail.com>

Signed-off-by: Martin K. Petersen <martin.petersen@oracle.com>

Diffstat

```
-rw-r--r-- drivers/scsi/lpfc/lpfc_init.c 2
-rw-r--r-- drivers/scsi/lpfc/lpfc_sli.c 4
```

2 files changed, 2 insertions, 4 deletions

diff --git a/drivers/scsi/lpfc/lpfc_init.c b/drivers/scsi/lpfc/lpfc_init.c
index 61958a24a43d9f..60e4ac2b8a6b3c 100644

--- a/drivers/scsi/lpfc/lpfc_init.c

+++ b/drivers/scsi/lpfc/lpfc_init.c

```
@@ -7291,6 +7291,8 @@ lpfc_sli4_cgn_params_read(struct lpfc_hba *phba)
    /* Find out if the FW has a new set of congestion parameters. */
    len = sizeof(struct lpfc_cgn_param);
    pdata = kzalloc(len, GFP_KERNEL);
+   if (!pdata)
+       return -ENOMEM;
    ret = lpfc_read_object(phba, (char *)LPFC_PORT_CFG_NAME,
                          pdata, len);
```

diff --git a/drivers/scsi/lpfc/lpfc_sli.c b/drivers/scsi/lpfc/lpfc_sli.c

index c5b69f313af365..c5ad46fdde8173 100644

--- a/drivers/scsi/lpfc/lpfc_sli.c

+++ b/drivers/scsi/lpfc/lpfc_sli.c

```
@@ -22109,10 +22109,6 @@ lpfc_read_object(struct lpfc_hba *phba, char *rdobject, uint32_t *datap,
    struct lpfc_dmabuf *pcmd;
    u32 rd_object_name[LPFC_MBX_OBJECT_NAME_LEN_DW] = {0};
```

```
-      /* sanity check on queue memory */  
-      if (!datap)  
-          return -ENODEV;  
-  
mbox = mempool_alloc(phba->mbox_mem_pool, GFP_KERNEL);  
if (!mbox)  
    return -ENOMEM;
```