



author Yang Yingliang <yangyingliang@huawei.com> 2022-11-07 20:48:28 +0800  
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-26 09:27:28 +0100  
commit [c736876ee294bb4f271d76a25cc7d70c8537bc5d](#) (patch)  
tree [7495dc007c21fb2ea1869b4adddea5e344499959](#)  
parent [a2282bd27fc97f8a65898f81d8abf7df41b8e4f7](#) (diff)  
download [linux-c736876ee294bb4f271d76a25cc7d70c8537bc5d.tar.gz](#)

**diff options**

context:  ▼  
space:  ▼  
mode:  ▼

**scsi: scsi\_transport\_sas: Fix error handling in sas\_phy\_add()**

[ Upstream commit 5d7bebf2dfb0dc97aac1fbace0910e557ecdb16f ]

If transport\_add\_device() fails in sas\_phy\_add(), the kernel will crash trying to delete the device in transport\_remove\_device() called from sas\_remove\_host().

Unable to handle kernel NULL pointer dereference at virtual address 0000000000000108  
CPU: 61 PID: 42829 Comm: rmmod Kdump: loaded Tainted: G W 6.1.0-rc1+ #173  
pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--)  
pc : device\_del+0x54/0x3d0  
lr : device\_del+0x37c/0x3d0  
Call trace:  
device\_del+0x54/0x3d0  
attribute\_container\_class\_device\_del+0x28/0x38  
transport\_remove\_classdev+0x6c/0x80  
attribute\_container\_device\_trigger+0x108/0x110  
transport\_remove\_device+0x28/0x38  
sas\_phy\_delete+0x30/0x60 [scsi\_transport\_sas]  
do\_sas\_phy\_delete+0x6c/0x80 [scsi\_transport\_sas]  
device\_for\_each\_child+0x68/0xb0  
sas\_remove\_children+0x40/0x50 [scsi\_transport\_sas]  
sas\_remove\_host+0x20/0x38 [scsi\_transport\_sas]  
hisi\_sas\_remove+0x40/0x68 [hisi\_sas\_main]  
hisi\_sas\_v2\_remove+0x20/0x30 [hisi\_sas\_v2\_hw]  
platform\_remove+0x2c/0x60

Fix this by checking and handling return value of transport\_add\_device() in sas\_phy\_add().

Fixes: [c7ebbbce366c](#) ("[SCSI] SAS transport class")  
Suggested-by: John Garry <john.g.garry@oracle.com>  
Signed-off-by: Yang Yingliang <yangyingliang@huawei.com>  
Link: <https://lore.kernel.org/r/20221107124828.115557-1-yangyingliang@huawei.com>  
Reviewed-by: John Garry <john.g.garry@oracle.com>  
Reviewed-by: Jason Yan <yanaijie@huawei.com>  
Signed-off-by: Martin K. Petersen <martin.petersen@oracle.com>  
Signed-off-by: Sasha Levin <sasha.l@kernel.org>

**Diffstat**

-rw-r--r-- [drivers/scsi/scsi\\_transport\\_sas.c](#) 13

1 files changed, 9 insertions, 4 deletions

```
diff --git a/drivers/scsi/scsi_transport_sas.c b/drivers/scsi/scsi_transport_sas.c
index 2f88c61216eea4..74b99f2b0b74ac 100644
--- a/drivers/scsi/scsi_transport_sas.c
+++ b/drivers/scsi/scsi_transport_sas.c
@@ -722,12 +722,17 @@ int sas_phy_add(struct sas_phy *phy)
    int error;

    error = device_add(&phy->dev);
-   if (!error) {
-       transport_add_device(&phy->dev);
-       transport_configure_device(&phy->dev);
+   if (error)
+       return error;
+
+   error = transport_add_device(&phy->dev);
+   if (error) {
+       device_del(&phy->dev);
+       return error;
+   }
+   transport_configure_device(&phy->dev);

-   return error;
+   return 0;
}
EXPORT_SYMBOL(sas_phy_add);
```