



author Yang Yingliang <yangyingliang@huawei.com> 2022-11-07 20:48:28 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-26 09:24:35 +0100
commit [2f21d653c648735657e23948b1d7ac7273de0f87](#) (patch)
tree [e2259e283fe8ba5c1aeaed8d62af434a8070ca89](#)
parent [7cd28bc410d2014447bae8db9de5e81297c01c03](#) (diff)
download [linux-2f21d653c648735657e23948b1d7ac7273de0f87.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: rmmmod 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 4a96fb05731d2f..c6256fdc24b10c 100644
--- a/drivers/scsi/scsi_transport_sas.c
+++ b/drivers/scsi/scsi_transport_sas.c
@@ -716,12 +716,17 @@ 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);
```