



author Yang Yingliang <yangyingliang@huawei.com> 2022-11-08 21:40:01 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:40:23 +0100
commit [30e12e2be27ac6c4be2af4163c70db381364706f](#) (patch)
tree [b6b7e6dfd55feedec108a3d1db4119c56f79907a](#)
parent [a988dcd3dd9e691c5ccc3324b209688f3b5453e9](#) (diff)
download [linux-30e12e2be27ac6c4be2af4163c70db381364706f.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

ata: libata-transpot: fix double ata_host_put() in ata_tport_add()

[Upstream commit 8c76310740807ade5ecdab5888f70ecb6d35732e]

In the error path in ata_tport_add(), when calling put_device(), ata_tport_release() is called, it will put the refcount of 'ap->host'.

And then ata_host_put() is called again, the refcount is decreased to 0, ata_host_release() is called, all ports are freed and set to null.

When unbinding the device after failure, ata_host_stop() is called to release the resources, it leads a null-ptr-deref(), because all the ports all freed and null.

Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008
CPU: 7 PID: 18671 Comm: modprobe Kdump: loaded Tainted: G E 6.1.0-rc3+ #8
pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=---)
pc : ata_host_stop+0x3c/0x84 [libata]
lr : release_nodes+0x64/0xd0
Call trace:
ata_host_stop+0x3c/0x84 [libata]
release_nodes+0x64/0xd0
devres_release_all+0xbc/0x1b0
device_unbind_cleanup+0x20/0x70
really_probe+0x158/0x320
__driver_probe_device+0x84/0x120
driver_probe_device+0x44/0x120
__driver_attach+0xb4/0x220
bus_for_each_dev+0x78/0xdc
driver_attach+0x2c/0x40
bus_add_driver+0x184/0x240
driver_register+0x80/0x13c
__pci_register_driver+0x4c/0x60
ahci_pci_driver_init+0x30/0x1000 [ahci]

Fix this by removing redundant ata_host_put() in the error path.

Fixes: 2623c7a5f279 ("libata: add refcounting to ata_host")
Signed-off-by: Yang Yingliang <yangyingliang@huawei.com>
Signed-off-by: Damien Le Moal <damien.lemoal@opensource.wdc.com>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

-rw-r--r-- drivers/ata/libata-transport.c	1
---	---

1 files changed, 0 insertions, 1 deletions

diff --git a/drivers/ata/libata-transport.c b/drivers/ata/libata-transport.c
index 43a91495ee6785..f04f4f977400da 100644

--- a/drivers/ata/libata-transport.c

+++ b/drivers/ata/libata-transport.c

```
@@ -317,7 +317,6 @@ int ata_tport_add(struct device *parent,
    tport_err:
        transport_destroy_device(dev);
        put_device(dev);
-       ata_host_put(ap->host);
        return error;
}
```