author	Shang XiaoJing <shangxiaojing@huawei.com>	2022-10-27 22:03:29 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-10 18:14:17 +0100
commit	e8c11ee2d07f7c4dfa2ac0ea8efc4f627e58ea57 (patch)	
tree	702776f12bb4687e7000e1e32c9b76fb26ef0d14	
parent	31b83d6990c8e5fe8600f4553bbe8beb2b249a56 (diff)	
download	linux-e8c11ee2d07f7c4dfa2ac0ea8efc4f627e58ea57.tar.gz	

nfc: fdp: Fix potential memory leak in fdp_nci_send()

```
[ Upstream commit 8e4aae6b8ca76afb1fb64dcb24be44ba814e7f8a ]

fdp_nci_send() will call fdp_nci_i2c_write that will not free skb in
the function. As a result, when fdp_nci_i2c_write() finished, the skb
will memleak. fdp_nci_send() should free skb after fdp_nci_i2c_write()
finished.

Fixes: a06347c04c13 ("NFC: Add Intel Fields Peak NFC solution driver")
Signed-off-by: Shang XiaoJing <shangxiaojing@huawei.com>
Signed-off-by: David S. Miller <davem@davemloft.net>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- drivers/nfc/fdp/fdp.c 10

1 files changed, 9 insertions, 1 deletions

```
diff --git a/drivers/nfc/fdp/fdp.c b/drivers/nfc/fdp/fdp.c
index 52c60d11849c23..90bea6a1db6921 100644
--- a/drivers/nfc/fdp/fdp.c
+++ b/drivers/nfc/fdp/fdp.c
@@ -252,11 +252,19 @@ static int fdp_nci_close(struct nci_dev *ndev)
 static int fdp_nci_send(struct nci_dev *ndev, struct sk_buff *skb)
 {
        struct fdp_nci_info *info = nci_get_drvdata(ndev);
+       int ret;

        if (atomic_dec_and_test(&info->data_pkt_counter))
                info->data_pkt_counter_cb(ndev);

-       return info->phy_ops->write(info->phy, skb);
+       ret = info->phy_ops->write(info->phy, skb);
+       if (ret < 0) {
+               kfree_skb(skb);
+               return ret;
+       }
+
+       consume_skb(skb);
+       return 0;
 }

 static int fdp_nci_request_firmware(struct nci_dev *ndev)
```