



# index : kernel/git/stable/linux.git

master



switch

Linux kernel stable tree

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg



search

author Shang XiaoJing <shangxiaojing@huawei.com> 2022-10-27 22:03:29 +0800  
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 18:15:27 +0100  
commit [44bc1868a4f542502ea2221fe5ad88ca66d1c6b6](#) (patch)  
tree [07d933f74af40232b07d6b9449db3cbc234c3362](#)  
parent [4bef9a89f2f563f8c19c86b4779f6152a5fff528](#) (diff)  
download [linux-44bc1868a4f542502ea2221fe5ad88ca66d1c6b6.tar.gz](#)

## diff options

context:

3



space:

include



mode:

unified



## 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 c6b3334f24c9ea..f12f903a9dd134 100644
--- a/drivers/nfc/fdp/fdp.c
+++ b/drivers/nfc/fdp/fdp.c
@@ -249,11 +249,19 @@ 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)
```