author	Shang XiaoJing <shangxiaojing@huawei.com>	2022-10-27 22:03:32 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-10 15:46:05 +0100
commit	dd0ee55ead91fbb16889dbe7ff0b0f7c9e4e849d (patch)	
tree	267f4649f4a17d7d4ad9ece179b11dba993bb8f6	
parent	8b149ab474f23703e85380e9f4437123ec7cfcc4 (diff)	
download	linux-dd0ee55ead91fbb16889dbe7ff0b0f7c9e4e849d.tar.gz	

nfc: nfcmrvl: Fix potential memory leak in nfcmrvl_i2c_nci_send()

```
[ Upstream commit 93d904a734a74c54d945a9884b4962977f1176cd ]

nfcmrvl_i2c_nci_send() will be called by nfcmrvl_nci_send(), and skb
should be freed in nfcmrvl_i2c_nci_send(). However, nfcmrvl_nci_send()
will only free skb when i2c_master_send() return >=0, which means skb
will memleak when i2c_master_send() failed. Free skb no matter whether
i2c_master_send() succeeds.

Fixes: b5b3e23e4cac ("NFC: nfcmrvl: add i2c 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/nfcmrvl/i2c.c 7

1 files changed, 6 insertions, 1 deletions

```
diff --git a/drivers/nfc/nfcmrvl/i2c.c b/drivers/nfc/nfcmrvl/i2c.c
index bb546cabe8090a..91d7ef11aba348 100644
--- a/drivers/nfc/nfcmrvl/i2c.c
+++ b/drivers/nfc/nfcmrvl/i2c.c
@@ -151,10 +151,15 @@ static int nfcmrvl_i2c_nci_send(struct nfcmrvl_private *priv,
                        ret = -EREMOTEIO;
                } else
                        ret = 0;
+       }
+
+       if (ret) {
                kfree_skb(skb);
+               return ret;
        }

-       return ret;
+       consume_skb(skb);
+       return 0;
 }

 static void nfcmrvl_i2c_nci_update_config(struct nfcmrvl_private *priv,
```