author	Zheng Wang <zyytlz.wz@163.com>	2023-03-13 00:08:37 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-22 13:27:09 +0100
commit	3405eb641dafcc8b28d174784b203c1622c121bf (patch)	
tree	865c87bbded2f116b6325fad1b878fc187864eab	
parent	cf98933ced59f298eefff9a03bf712d24efa1e98 (diff)	
download	linux-3405eb641dafcc8b28d174784b203c1622c121bf.tar.gz	

nfc: st-nci: Fix use after free bug in ndlc_remove due to race condition

```
[ Upstream commit 5000fe6c27827a61d8250a7e4a1d26c3298ef4f6 ]

This bug influences both st_nci_i2c_remove and st_nci_spi_remove.
Take st_nci_i2c_remove as an example.

In st_nci_i2c_probe, it called ndlc_probe and bound &ndlc->sm_work
with llt_ndlc_sm_work.

When it calls ndlc_recv or timeout handler, it will finally call
schedule_work to start the work.

When we call st_nci_i2c_remove to remove the driver, there
may be a sequence as follows:

Fix it by finishing the work before cleanup in ndlc_remove

CPU0                  CPU1

                     |llt_ndlc_sm_work
st_nci_i2c_remove    |
  ndlc_remove        |
    st_nci_remove    |
    nci_free_device  |
    kfree(ndev)      |
//free ndlc->ndev    |
                     |llt_ndlc_rcv_queue
                     |nci_recv_frame
                     |//use ndlc->ndev

Fixes: 35630df68d60 ("NFC: st21nfcb: Add driver for STMicroelectronics ST21NFCB NFC chip")
Signed-off-by: Zheng Wang <zyytlz.wz@163.com>
Reviewed-by: Krzysztof Kozlowski <krzysztof.kozlowski@linaro.org>
Link: https://lore.kernel.org/r/20230312160837.2040857-1-zyytlz.wz@163.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- drivers/nfc/st-nci/ndlc.c 6

1 files changed, 4 insertions, 2 deletions

```
diff --git a/drivers/nfc/st-nci/ndlc.c b/drivers/nfc/st-nci/ndlc.c
index f26d938d240f03..12d73f9dbe9f37 100644
--- a/drivers/nfc/st-nci/ndlc.c
+++ b/drivers/nfc/st-nci/ndlc.c
@@ -297,13 +297,15 @@ EXPORT_SYMBOL(ndlc_probe);

 void ndlc_remove(struct llt_ndlc *ndlc)
 {
-       st_nci_remove(ndlc->ndev);
-
        /* cancel timers */
        del_timer_sync(&ndlc->t1_timer);
        del_timer_sync(&ndlc->t2_timer);
        ndlc->t2_active = false;
        ndlc->t1_active = false;
+       /* cancel work */
+       cancel_work_sync(&ndlc->sm_work);
+
+       st_nci_remove(ndlc->ndev);

        skb_queue_purge(&ndlc->rcv_q);
        skb_queue_purge(&ndlc->send_q);
```