

libosmcore - Bug #1761

LAPD: segfault when bootstrapping Nokia InSite

07/03/2016 08:17 PM - laforge

Status: New	Start date: 07/03/2016
Priority: Normal	Due date:
Assignee:	% Done: 20%
Category:	
Target version:	
Spec Reference:	
Description	
When bootstrapping a Nokia InSite BTS, current OsmonITB segfaults.	
The reason for this is as follows:	
<ul style="list-style-type: none">• ABM is established.• LAPD code hands an I frame to the application using send_dl_l3()• user application decides to call lapd_sap_stop() resulting in a local RELEASE request to LAPD• LAPD clears the transmit history and changes to IDLE state• application returns from processing the I frame• code proceeds in lapd_rx_i() and tries to transmit an I frame, as it didn't realize the state has meanwhile changed• lapd_send_i() tries to use dl->tx_hist -> boom.	
As this is the second bug related to accessing a free'd tx_hist, the code seems to require a more thorough audit.	
Related issues:	
Related to libosmcore - Bug #1760: LAPD: segfault in T200 call-back	Closed 07/03/2016
Related to libosmcore - Bug #1762: Review LAPD code for race conditions rega...	New 07/03/2016

History

#1 - 07/03/2016 08:17 PM - laforge

- Related to Bug #1760: LAPD: segfault in T200 call-back added

#2 - 07/03/2016 08:19 PM - laforge

- Status changed from New to In Progress

- % Done changed from 0 to 20

The quick fix for this specific bug is to check for LAPD_STATE_MF_EST in the first lines of labd_send_i(), and return if not. Not sure how many other similar bugs are still hidden :/

#3 - 07/03/2016 08:20 PM - laforge

- Related to Bug #1762: Review LAPD code for race conditions regarding state, particularly in RELEASE added

#4 - 11/09/2016 10:20 AM - laforge

- Assignee deleted (laforge)

#5 - 10/05/2017 06:27 AM - laforge

- Status changed from In Progress to New