OsmoMSC - Bug #4117

osmo-msc crash when paging SGs after MME disconnects

07/17/2019 11:26 PM - laforge

Status:	New	**Start date:**	07/18/2019
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	0%
Category:	SGs Interface		
Target version:			
Resolution:			

Description

from the nextepc mailing list:

> I some situations, when the MME lost connection with the OSMO-MSC and return this connection if I try send a MT-CSFB the OSMO-MSC is crashing.
>
> I get this error in the log:
>
> <0006> sgs_iface.c:470 XXXXXXXXXX state 1 conf_by_radio_contact_ind 1
> <0011> sgs_iface.c:251 (sub IMSI-724210000000003:MSISDN-5544912340003:TMSI-0x8E44F269) Tx PAGING-REQUEST suitable MME found, but no SGS connection present!
> <0005> sgs_iface.c:480 SGs-UE[0x563949b08fc0]{SGs-ASSOCIATED}: Will not Page (no MME)
> <0005> paging.c:101 Paging: IMSI-724210000000003:MSISDN-5544912340003:TMSI-0x8E44F269 for MNCC: establish call: Starting paging failed (rc=-22)
> <0001> gsm_04_08_cc.c:1922 trans(CC IMSI-724210000000003:MSISDN-5544912340003:TMSI-0x8E44F269 callref-0x1396 tid-255) Failed to allocate paging token.
> Segmentation fault (core dumped)

History

#1 - 07/17/2019 11:29 PM - laforge

- File saida98csfb.pcap added

See http://lists.osmocom.org/pipermail/nextepc/2019-July/000071.html for the original post

#2 - 07/18/2019 01:07 AM - medeiros405

- File backtrace.txt added

Hello,

Running the OSMO-MSC in debug mode like Harald ask me I get this message:

Program received signal SIGSEGV, Segmentation fault.
0x00005555555957c9 in msc_a_tx_dtap_to_i (msc_a=0x0, dtap=0x5555559acd40) at msc_a.c:1560
1560 if (msc_a->c.ran->type == OSMO_RAT_EUTRAN_SGS) {
(gdb)
(gdb)
(gdb)

The backtrace full is in attached.

Thanks

Romeu Medeiros

#3 - 08/01/2019 09:27 AM - dexter

Hello.

I have done some experiments in order to see if I can reproduce this. I have made sure that the UE was camping on my LTE test network. Then I have terminated the MME process and tried to initiate a call to the UE. This did not crash the MSC. Also attempting to terminate the MME did not work for me. I do not see any SGSAP activity in the pcap file, so it is more likely that the crash occurs with a paging that is initiated after the MME has been disconnected.

I suggest to try with current master of osmo-msc. It would be also good to have a detailed description of the circumstances under which the crash occurs.

Best regards.
Philipp

Files

saida98csfb.pcap	17 KB	07/17/2019	laforge
backtrace.txt	39.9 KB	07/18/2019	medeiros405