osmo-sip-connector - Bug #4159

osmo-sip-connector segfaults

08/20/2019 11:38 AM - dexter

Status:	Resolved	**Start date:**	08/20/2019
Priority:	Normal	**Due date:**	
Assignee:	dexter	**% Done:**	100%
Category:			
Target version:			
Resolution:			

Description

```
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:956 MNCC rcvd message type: MNCC_DISC_IND
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:575 Rcvd MNCC_DISC_IND, Cause: NORM_CALL_CLEAR
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:577 leg(2147483649) was disconnected. Releasing
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:68 Starting Timer for MNCC_REL_CNF
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:142 MNCC sent message type: MNCC_REL_REQ
Tue Aug 20 13:16:12 2019 DSIP <0000> sip.c:457 sip_release_call(): Release with MNCC cause(NORM_CA
LL_CLEAR)
Tue Aug 20 13:16:12 2019 DSIP <0000> sip.c:429 cause2status(): Mapping cause(NORM_CALL_CLEAR) to s
tatus(200)
Tue Aug 20 13:16:12 2019 DSIP <0000> sip.c:481 Ending leg(0x55d0078bb090) in connected state.
Tue Aug 20 13:16:12 2019 DSIP <0000> sip.c:327 SIP event[nua_r_bye] status(200) phrase(OK) 0x55d00
78bb090
Tue Aug 20 13:16:12 2019 DSIP <0000> sip.c:376 leg(0x55d0078bb090) got resp to bye
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:956 MNCC rcvd message type: MNCC_REL_CNF
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:82 Got response(MNCC_REL_CNF), stopping timer on leg(
2147483649)
Tue Aug 20 13:16:12 2019 DMNCC <0001> mncc.c:624 leg(2147483649) was cnf released.
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:327 SIP event[nua_i_invite] status(100) phrase(Trying)
(nil)
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:392 Processing INVITE Call-ID: 6deb60a42abf482b0f4555df
2a0e06fb@10.9.1.122:5060
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:115 Incoming call(6deb60a42abf482b0f4555df2a0e06fb@10.9
.1.122:5060) handle(0x55d0078bfaf0)
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:167 SDP Extracted: IP=(10.9.1.122) PORT=(14472) PAYLOAD
=(3).
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:327 SIP event[nua_i_state] status(100) phrase(Trying) 0
x55d0078c2170
Tue Aug 20 13:24:18 2019 DSIP <0000> sip.c:415 Did not handle event[nua_i_state] status(100)
Tue Aug 20 13:24:21 2019 DMNCC <0001> mncc.c:946 Failed to read 0/Function not implemented. Re-con
necting.
Tue Aug 20 13:24:21 2019 DAPP <0002> app.c:50 Going to release call(5020) due MNCC.
Tue Aug 20 13:24:21 2019 DSIP <0000> sip.c:457 sip_release_call(): Release with MNCC cause(unknown
 0x0)
Tue Aug 20 13:24:21 2019 DSIP <0000> sip.c:433 cause2status(): Cause(unknown 0x0) not found in map
.
Tue Aug 20 13:24:21 2019 DSIP <0000> sip.c:468 Cancelling leg(0x55d0078c2170) in confirmed state
Tue Aug 20 13:24:21 2019 DMNCC <0001> mncc.c:290 MNCC not connected releasing leg(5020)
Tue Aug 20 13:24:26 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:31 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:36 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:41 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:46 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:51 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:24:56 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:25:01 2019 DMNCC <0001> mncc.c:925 Failed to connect(/tmp/bsc_mncc). Retrying
Tue Aug 20 13:25:04 2019 DSIP <0000> sip.c:327 SIP event[nua_i_invite] status(100) phrase(Trying)
(nil)
Tue Aug 20 13:25:04 2019 DSIP <0000> sip.c:392 Processing INVITE Call-ID: 2465a4853348db406e3bd1d6
18d95ce8@10.9.1.122:5060
Tue Aug 20 13:25:04 2019 DSIP <0000> sip.c:115 Incoming call(2465a4853348db406e3bd1d618d95ce8@10.9
.1.122:5060) handle(0x55d0078bd160)
```

```
Tue Aug 20 13:25:04 2019 DSIP <0000> sip.c:167 SDP Extracted: IP=(10.9.1.122) PORT=(15736) PAYLOAD
=(3).
Tue Aug 20 13:25:04 2019 DMNCC <0001> mncc.c:906 Failed to send message leg(5021)
./start-osmo-sip-connector.sh: line 5: 20158 Segmentation fault      sudo osmo-sip-connector -c ./
osmo-sip-connector.cfg
```

History

#1 - 08/20/2019 11:41 AM - dexter

The crash might be related to a crash of osmo-msc: https://osmocom.org/issues/4160

#2 - 08/28/2019 12:23 PM - dexter

- File core.22903 added

Apparently the crash can be provoked when osmo-msc is terminated and a call to an MS is made via sip landline. Then osmo-sip-connector should crash.

```
#0  osmo_fd_unregister (fd=fd@entry=0x555555762b68 <g_app+104>) at select.c:141
#1  0x000055555555a90d in close_connection (conn=0x555555762b58 <g_app+88>) at mncc.c:327
#2  0x000055555555cb5c in mncc_create_remote_leg (conn=0x555555762b58 <g_app+88>, call=call@entry=0x55555580b6
90) at mncc.c:907
#3  0x00005555555588fa in route_to_mncc (call=0x55555580b690) at app.c:77
#4  app_route_call (call=call@entry=0x55555580b690, source=0x55555580d180 "2600", dest=dest@entry=0x55555580ad
10 "23001") at app.c:97
#5  0x0000555555559fee in new_call (sip=0x555555807e58, nh=0x55555580a160, agent=0x555555762b20 <g_app+32>) at
 sip.c:180
#6  nua_callback (event=<optimized out>, status=<optimized out>, phrase=<optimized out>, nua=<optimized out>,
magic=0x555555762b20 <g_app+32>, nh=0x55555580a160, hmagic=0x0, sip=0x555555807e58, tags=0x55555580b5a0) at si
p.c:399
#7  0x00007ffff78efc34 in ?? () from /usr/lib/libsofia-sip-ua.so.0
#8  0x00007ffff7940362 in ?? () from /usr/lib/libsofia-sip-ua.so.0
#9  0x00007ffff7bd5e50 in ?? () from /usr/lib/libsofia-sip-ua-glib.so.3
#10 0x00007ffff757a7f7 in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#11 0x00007ffff757aa60 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#12 0x00007ffff757ad82 in g_main_loop_run () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#13 0x0000555555557e0c in main (argc=3, argv=0x7fffffffe208) at main.c:184

#0  osmo_fd_unregister (fd=fd@entry=0x555555762b68 <g_app+104>) at select.c:141
No locals.
#1  0x000055555555a90d in close_connection (conn=0x555555762b58 <g_app+88>) at mncc.c:327
No locals.
#2  0x000055555555cb5c in mncc_create_remote_leg (conn=0x555555762b58 <g_app+88>, call=call@entry=0x55555580b6
90) at mncc.c:907
        leg = 0x55555580d1f0
        mncc = {msg_type = 257, callref = 5012, fields = 6, bearer_cap = {transfer = 0, mode = 0, coding = 0,
radio = 0, speech_ctm = 0, speech_ver = {0, 0, 0, 0, 0, 0, 0, 0}, data = {rate_adaption = GSM48_BCAP_RA_NONE,
sig_access = 0, async = 0, nr_stop_bits = 0,
             nr_data_bits = 0, user_rate = 0, parity = GSM48_BCAP_PAR_ODD, interm_rate = 0, transp = GSM48_BC
AP_TR_TRANSP, modem_type = GSM48_BCAP_MT_NONE}}, called = {type = 0, plan = 1, present = 0, screen = 0, number
 = "23001", '\000' <repeats 27 times>},
          calling = {type = 0, plan = 1, present = 0, screen = 0, number = "2600", '\000' <repeats 28 times>},
 redirecting = {type = 0, plan = 0, present = 0, screen = 0, number = '\000' <repeats 32 times>}, connected =
{type = 0, plan = 0, present = 0, screen = 0,
            number = '\000' <repeats 32 times>}, cause = {location = 0, coding = 0, rec = 0, rec_val = 0, valu
e = 0, diag_len = 0, diag = '\000' <repeats 31 times>}, progress = {coding = 0, location = 0, descr = 0}, user
user = {proto = 0,
            info = '\000' <repeats 128 times>}, facility = {len = 0, info = '\000' <repeats 127 times>}, cccap
 = {dtmf = 0, pcp = 0}, ssversion = {len = 0, info = '\000' <repeats 127 times>}, clir = {sup = 0, inv = 0}, s
ignal = 0, keypad = 0, more = 0, notify = 0,
          emergency = 0, imsi = '\000' <repeats 15 times>, lchan_type = 0 '\000', lchan_mode = 0 '\000'}
        rc = <optimized out>
#3  0x00005555555588fa in route_to_mncc (call=0x55555580b690) at app.c:77
No locals.
#4  app_route_call (call=call@entry=0x55555580b690, source=0x55555580d180 "2600", dest=dest@entry=0x55555580ad
10 "23001") at app.c:97
No locals.
#5  0x0000555555559fee in new_call (sip=0x555555807e58, nh=0x55555580a160, agent=0x555555762b20 <g_app+32>) at
 sip.c:180
        call = 0x55555580b690
        from = 0x5555558083bd "2600"
        ip_addr = "10.9.1.122\000UUU\000"
```

```
        net = {s_addr = 2046888202}
        leg = 0x55555580cf60
        to = <optimized out>
#6  nua_callback (event=<optimized out>, status=<optimized out>, phrase=<optimized out>, nua=<optimized out>,
magic=0x555555762b20 <g_app+32>, nh=0x55555580a160, hmagic=0x0, sip=0x555555807e58, tags=0x55555580b5a0) at si
p.c:399
        leg = <optimized out>
#7  0x00007ffff78efc34 in ?? () from /usr/lib/libsofia-sip-ua.so.0
No symbol table info available.
#8  0x00007ffff7940362 in ?? () from /usr/lib/libsofia-sip-ua.so.0
No symbol table info available.
#9  0x00007ffff7bd5e50 in ?? () from /usr/lib/libsofia-sip-ua-glib.so.3
No symbol table info available.
#10 0x00007ffff757a7f7 in g_main_context_dispatch () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
No symbol table info available.
#11 0x00007ffff757aa60 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
No symbol table info available.
#12 0x00007ffff757ad82 in g_main_loop_run () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
No symbol table info available.
#13 0x0000555555557e0c in main (argc=3, argv=0x7fffffffe208) at main.c:184
        rc = <optimized out>
        loop = 0x555555763e60
```

#3 - 08/28/2019 01:16 PM - dexter

- Status changed from New to In Progress

- % Done changed from 0 to 90

I have investigated this and I found out that close_connection() does call osmo_fd_unregister(). For some reason the osmo-fd is not registered in this special case. Lets check using osmo_fd_is_registered() before we unregister the fd.

See also: https://gerrit.osmocom.org/c/osmo-sip-connector/+/15303 mncc: do not unregister unregistered osmo fds

#4 - 09/04/2019 09:23 AM - laforge

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

patch was merged

Files

core.22903	1.86 MB	08/28/2019	dexter