OsmoGSMTester - Bug #4542

ofono: crash in drivers/qmimodem/gprs.c:extract_ss_info()

05/11/2020 10:09 AM - pespin

Status:	Feedback	**Start date:**	05/11/2020
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

```
------------------------------------------------
trial-2115 nitb_smpp esme_ms_sms_transaction.py
------------------------------------------------
23:41:26.470917 tst                          nitb_smpp: Using 1 x ip_address (candidates: 1)
23:41:26.485698 tst                          nitb_smpp: Using 1 x bts (candidates: 1)
23:41:28.228938 tst       esme_ms_sms_transaction.py: using LAC 8882
23:41:28.343204 tst       esme_ms_sms_transaction.py: using RAC 212
23:41:28.454695 tst       esme_ms_sms_transaction.py: using CellId 8882
23:41:28.566672 tst       esme_ms_sms_transaction.py: using BVCI 8883
23:41:28.671100 tst                          nitb_smpp: Using 1 x modem (candidates: 1)
23:41:28.705811 tst    esme_ms_sms_transaction.py:15: ERR: Error: g-dbus-error-quark: GDBus.Error:
org.freedesktop.DBus.Error.ServiceUnknown: The name org.ofono was not provided by any .service fil
es (2)  [trial-2115↬nitb_smpp↬esme_ms_sms_transaction.py:15]
23:41:28.715436 tst    esme_ms_sms_transaction.py:15: Test FAILED (2.2 sec)

/usr/local/sbin/ofonod --version
1.31
```

So ofono version is our osmo-gsm-tester branch of ofono.git (git.sysmocom.de) currently based on top of upstream 1.31 release.
https://git.sysmocom.de/ofono/commit/?h=osmo-gsm-tester&id=73e7f8bec0c3dd77dc4f41ee7bd9fa3275f94a39

ofono is crashing a lot lately when using modems to run gprs related tests:

```
May 10 23:41:08.612586 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:get_ss_info_cb(
)
May 10 23:41:08.612612 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:handle_ss_info(
)
May 10 23:41:08.612635 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:extract_ss_info
()
May 10 23:41:08.612659 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:extract_ss_info
() radio in use 4
May 10 23:41:08.612685 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:registration_status_cb() /go
bi_2 error 0 status 1
May 10 23:41:08.612711 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:ofono_gprs_status_notify() /
gobi_2 status registered (1)
May 10 23:41:08.612736 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:qmi_set_attache
d() attached 0
May 10 23:41:08.612901 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
_REQ: QMI QMUX:
                                                           QMI   length  = 16
                                                           QMI   flags   = 0x00
                                                           QMI   service = "nas"
                                                           QMI   client  = 3
                                                           QMI QMI:
                                                           QMI   flags       = "none"
                                                           QMI   transaction = 339
                                                           QMI   tlv_length  = 4
                                                           QMI   message     = (0x0023)
                                                           QMI TLV:
                                                           QMI   type    = 0x10
```

```
                                                    QMI   length = 1
                                                    QMI   value  = 02
May 10 23:41:08.754412 osmo-gsm-tester-prod ofonod[22747]: src/modem.c:get_modem_property() modem
0x55eab5d78930 property AlwaysOnline
May 10 23:41:08.754483 osmo-gsm-tester-prod ofonod[22747]: plugins/gobi.c:gobi_set_online() 0x55ea
b5d78930 offline
May 10 23:41:08.754755 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
_REQ: QMI QMUX:
                                                    QMI   length  = 16
                                                    QMI   flags   = 0x00
                                                    QMI   service = "dms"
                                                    QMI   client  = 4
                                                    QMI QMI:
                                                    QMI   flags       = "none"
                                                    QMI   transaction = 340
                                                    QMI   tlv_length  = 4
                                                    QMI   message     = "Set Operating Mode
" (0x002E)
                                                    QMI TLV:
                                                    QMI   type       = "Mode" (0x01)
                                                    QMI   length     = 1
                                                    QMI   value      = 01
                                                    QMI   translated = low-power
May 10 23:41:11.428304 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
READ: QMI QMUX:
                                                    QMI   length  = 19
                                                    QMI   flags   = 0x80
                                                    QMI   service = "nas"
                                                    QMI   client  = 3
                                                    QMI QMI:
                                                    QMI   flags       = "response"
                                                    QMI   transaction = 339
                                                    QMI   tlv_length  = 7
                                                    QMI   message     = (0x0023)
                                                    QMI TLV:
                                                    QMI   type   = 0x02
                                                    QMI   length = 4
                                                    QMI   value  = 00:00:00:00
May 10 23:41:11.428369 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:attach_detach_c
b()
May 10 23:41:11.428397 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_attach_callback() /gobi
_2 error = 0
May 10 23:41:11.428424 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:qmi_attached_st
atus()
May 10 23:41:11.428580 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
_REQ: QMI QMUX:
                                                    QMI   length  = 12
                                                    QMI   flags   = 0x00
                                                    QMI   service = "nas"
                                                    QMI   client  = 3
                                                    QMI QMI:
                                                    QMI   flags       = "none"
                                                    QMI   transaction = 341
                                                    QMI   tlv_length  = 0
                                                    QMI   message     = "Get Serving System
" (0x0024)
May 10 23:41:11.460431 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
READ: QMI QMUX:
                                                    QMI   length  = 19
                                                    QMI   flags   = 0x80
                                                    QMI   service = "dms"
                                                    QMI   client  = 4
                                                    QMI QMI:
                                                    QMI   flags       = "response"
                                                    QMI   transaction = 340
                                                    QMI   tlv_length  = 7
                                                    QMI   message     = "Set Operating Mode
```

```
" (0x002E)
                                                    QMI TLV:
                                                    QMI   type       = "Result" (0x02)
                                                    QMI   length     = 4
                                                    QMI   value      = 00:00:00:00
                                                    QMI   translated = SUCCESS
May 10 23:41:11.460495 osmo-gsm-tester-prod ofonod[22747]: plugins/gobi.c:set_online_cb()
May 10 23:41:11.460882 osmo-gsm-tester-prod ofonod[22747]: src/modem.c:modem_change_state() old st
ate: 3, new state: 2
May 10 23:41:11.460906 osmo-gsm-tester-prod ofonod[22747]: src/modem.c:flush_atoms()
May 10 23:41:11.460938 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_context_unregister() 0x
55eab5deb320, 0x55eab5deb100
May 10 23:41:11.460967 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_context_remove() atom:
0x55eab5deb360
May 10 23:41:11.460998 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs-context.c:qmi_gpr
s_context_remove()
May 10 23:41:11.461078 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_unregister() 0x55eab5de
b100
May 10 23:41:11.473859 osmo-gsm-tester-prod ofonod[22747]: src/network.c:__ofono_netreg_remove_sta
tus_watch() 0x55eab5eee220
May 10 23:41:11.473929 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_remove() atom: 0x55eab5
deb1b0
May 10 23:41:11.473998 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:qmi_gprs_remove
()
May 10 23:41:11.474049 osmo-gsm-tester-prod ofonod[22747]: src/ussd.c:ussd_remove() atom: 0x55eab5
e8a0f0
May 10 23:41:11.474069 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/ussd.c:qmi_ussd_remove
()
May 10 23:41:11.474109 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/netmon.c:qmi_netmon_re
move()
May 10 23:41:11.482561 osmo-gsm-tester-prod ofonod[22747]: src/sim.c:ofono_sim_remove_spn_watch()
0x55eab5e73700
May 10 23:41:11.482636 osmo-gsm-tester-prod ofonod[22747]: src/network.c:netreg_remove() atom: 0x5
5eab5eee120
May 10 23:41:11.482657 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/network-registration.c
:qmi_netreg_remove()
May 10 23:41:11.482901 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
_REQ: QMI QMUX:
                                                    QMI   length  = 16
                                                    QMI   flags   = 0x00
                                                    QMI   service = "ctl"
                                                    QMI   client  = 0
                                                    QMI QMI:
                                                    QMI   flags       = "none"
                                                    QMI   transaction = 11
                                                    QMI   tlv_length  = 5
                                                    QMI   message     = "Release CID" (0x00
23)
                                                    QMI TLV:
                                                    QMI   type       = "Release Info" (0x01
)
                                                    QMI   length     = 2
                                                    QMI   value      = 1A:01
                                                    QMI   translated = [ service = 'wda' ci
d = '1' ]
May 10 23:41:11.494316 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi()
READ: QMI QMUX:
                                                    QMI   length  = 94
                                                    QMI   flags   = 0x80
                                                    QMI   service = "nas"
                                                    QMI   client  = 3
                                                    QMI QMI:
                                                    QMI   flags       = "response"
                                                    QMI   transaction = 341
                                                    QMI   tlv_length  = 82
                                                    QMI   message     = "Get Serving System
" (0x0024)
```

```
                                                    QMI TLV:
                                                    QMI   type       = "Result" (0x02)
                                                    QMI   length     = 4
                                                    QMI   value      = 00:00:00:00
                                                    QMI   translated = SUCCESS
                                                    QMI TLV:
                                                    QMI   type       = "MNC PCS Digit Inclu
de Status" (0x27)
                                                    QMI   length     = 5
                                                    QMI   value      = 85:03:46:00:00
                                                    QMI   translated = [ mcc = '901' mnc =
'70' includes_pcs_digit = 'no' ]
                                                    QMI TLV:
                                                    QMI   type       = "Call Barring Status
" (0x25)
                                                    QMI   length     = 8
                                                    QMI   value      = 00:00:00:00:00:00:00
:00
                                                    QMI   translated = [ cs_status = 'norma
l-only' ps_status = 'normal-only' ]
                                                    QMI TLV:
                                                    QMI   type       = "Detailed Service St
atus" (0x21)
                                                    QMI   length     = 5
                                                    QMI   value      = 02:03:04:01:00
                                                    QMI   translated = [ status = 'availabl
e' capability = 'cs-ps' hdr_status = 'power-save' hdr_hybrid = 'yes' forbidden = 'no' ]
                                                    QMI TLV:
                                                    QMI   type       = "DTM Support" (0x20)
                                                    QMI   length     = 1
                                                    QMI   value      = 00
                                                    QMI   translated = no
                                                    QMI TLV:
                                                    QMI   type       = "CID 3GPP" (0x1d)
                                                    QMI   length     = 4
                                                    QMI   value      = B0:22:00:00
                                                    QMI   translated = 8880
                                                    QMI TLV:
                                                    QMI   type       = "LAC 3GPP" (0x1c)
                                                    QMI   length     = 2
                                                    QMI   value      = B0:22
                                                    QMI   translated = 8880
                                                    QMI TLV:
                                                    QMI   type       = "Roaming Indicator L
ist" (0x15)
                                                    QMI   length     = 3
                                                    QMI   value      = 01:04:01
                                                    QMI   translated = { [0] = '[ radio_int
erface = 'gsm' roaming_indicator = 'off' ] '}
                                                    QMI TLV:
                                                    QMI   type       = "Current PLMN" (0x12
)
                                                    QMI   length     = 5
                                                    QMI   value      = 85:03:46:00:00
                                                    QMI   translated = [ mcc = '901' mnc =
'70' description = '' ]
                                                    QMI TLV:
                                                    QMI   type       = "Data Service Capabi
lity" (0x11)
                                                    QMI   length     = 2
                                                    QMI   value      = 01:01
                                                    QMI   translated = { [0] = 'gprs '}
                                                    QMI TLV:
                                                    QMI   type       = "Roaming Indicator"
(0x10)
                                                    QMI   length     = 1
                                                    QMI   value      = 01
```

```
                                                    QMI   translated = off
                                                    QMI TLV:
                                                    QMI   type       = "Serving System" (0x
01)
                                                    QMI   length     = 6
                                                    QMI   value      = 01:01:01:02:01:04
                                                    QMI   translated = [ registration_state
 = 'registered' cs_attach_state = 'attached' ps_attach_state = 'attached' selected_network = '3gpp
' radio_interfaces = '{ [0] = 'gsm '}' ]
May 10 23:41:11.494370 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:get_ss_info_cb(
)
May 10 23:41:11.494391 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:handle_ss_info(
)
May 10 23:41:11.494410 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:extract_ss_info
()
May 10 23:41:11.494430 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:extract_ss_info
() radio in use 4
May 10 23:41:11.494475 osmo-gsm-tester-prod ofonod[22747]: Aborting (signal 11) [/usr/local/sbin/o
fonod]
May 10 23:41:11.496177 osmo-gsm-tester-prod ofonod[22747]: ++++++++ backtrace ++++++++
May 10 23:41:11.517527 osmo-gsm-tester-prod ofonod[22747]: #0  0x7fe57ef27060 in /lib/x86_64-linux
-gnu/libc.so.6
May 10 23:41:11.532526 osmo-gsm-tester-prod systemd[1]: ofono.service: Main process exited, code=e
xited, status=1/FAILURE
May 10 23:41:11.535204 osmo-gsm-tester-prod systemd[1]: ofono.service: Unit entered failed state.
May 10 23:41:11.535321 osmo-gsm-tester-prod systemd[1]: ofono.service: Failed with result 'exit-co
de'.
May 10 23:41:13.766647 osmo-gsm-tester-prod systemd[1]: ofono.service: Service hold-off time over,
 scheduling restart.
May 10 23:41:13.767895 osmo-gsm-tester-prod systemd[1]: Stopped Telephony service.
May 10 23:41:13.775458 osmo-gsm-tester-prod systemd[1]: Starting Telephony service..
```

History

#1 - 05/11/2020 10:20 AM - pespin

- Description updated

#2 - 05/11/2020 10:53 AM - pespin

Looks like a race condition. The usual scenario, (working non-crashing one) is to call qmi_attached_status() and then receive the callback from modem in get_ss_info_cb().
However, in some cases (crashing ones) we receive some events in between qmi_attached_status() and receiving the callback in get_ss_info_cb().
For intance:

```
May 10 23:41:11.428424 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:qmi_attached_status()
...
May 10 23:41:11.460495 osmo-gsm-tester-prod ofonod[22747]: plugins/gobi.c:set_online_cb()
May 10 23:41:11.460882 osmo-gsm-tester-prod ofonod[22747]: src/modem.c:modem_change_state() old state: 3, new
state: 2
May 10 23:41:11.460906 osmo-gsm-tester-prod ofonod[22747]: src/modem.c:flush_atoms()
May 10 23:41:11.460938 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_context_unregister() 0x55eab5deb320
, 0x55eab5deb100
May 10 23:41:11.460967 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_context_remove() atom: 0x55eab5deb3
60
May 10 23:41:11.460998 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs-context.c:qmi_gprs_context_re
move()
May 10 23:41:11.461078 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_unregister() 0x55eab5deb100
May 10 23:41:11.473859 osmo-gsm-tester-prod ofonod[22747]: src/network.c:__ofono_netreg_remove_status_watch()
0x55eab5eee220
May 10 23:41:11.473929 osmo-gsm-tester-prod ofonod[22747]: src/gprs.c:gprs_remove() atom: 0x55eab5deb1b0
May 10 23:41:11.473998 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:qmi_gprs_remove()
May 10 23:41:11.474049 osmo-gsm-tester-prod ofonod[22747]: src/ussd.c:ussd_remove() atom: 0x55eab5e8a0f0
May 10 23:41:11.474069 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/ussd.c:qmi_ussd_remove()
May 10 23:41:11.474109 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/netmon.c:qmi_netmon_remove()
May 10 23:41:11.482561 osmo-gsm-tester-prod ofonod[22747]: src/sim.c:ofono_sim_remove_spn_watch() 0x55eab5e737
00
May 10 23:41:11.482636 osmo-gsm-tester-prod ofonod[22747]: src/network.c:netreg_remove() atom: 0x55eab5eee120
May 10 23:41:11.482657 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/network-registration.c:qmi_netreg_
```

```
remove()
May 10 23:41:11.482901 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/qmibridge.c:ask_qmi() _REQ: QMI QM
UX:
                                                    QMI   length  = 16
                                                    QMI   flags   = 0x00
                                                    QMI   service = "ctl"
                                                    QMI   client  = 0
                                                    QMI QMI:
                                                    QMI   flags       = "none"
                                                    QMI   transaction = 11
                                                    QMI   tlv_length  = 5
                                                    QMI   message     = "Release CID" (0x0023)
                                                    QMI TLV:
                                                    QMI   type       = "Release Info" (0x01)
                                                    QMI   length     = 2
                                                    QMI   value      = 1A:01
                                                    QMI   translated = [ service = 'wda' cid = '1' ]
AND FINALLY WE RECEIVE OUR RESPONSE WHICH WILL CRASH:
May 10 23:41:11.494370 osmo-gsm-tester-prod ofonod[22747]: drivers/qmimodem/gprs.c:get_ss_info_cb()
```

So probably some stuff which is used in the callback is being de-allocated due to "modem_change_state() old state: 3, new state: 2" (MODEM_STATE_ONLINE -> MODEM_STATE_OFFLINE).

#3 - 05/11/2020 11:40 AM - pespin

So in qmi_attached_status(), "struct ofono_gprs *gprs" is assigned to "cbd->user = gprs;" to be used later during get_ss_info_cb() callback.

Then while we wait for callback in gprs_remove(), "struct ofono_gprs" is freed:

```
struct ofono_gprs *gprs = __ofono_atom_get_data(atom);
    if (gprs->driver && gprs->driver->remove)
        gprs->driver->remove(gprs);

    g_free(gprs);
```

And finally callback get_ss_info_cb() arrives and uses it:

```
struct ofono_gprs *gprs = cbd->user;
status = handle_ss_info(result, gprs);

// In handle_ss_info() gprs is derreferenced and probably crashes when setting the value:
struct gprs_data *data = ofono_gprs_get_data(gprs);
...
data->last_auto_context_id = 0;  <--- crash here.
```

#4 - 05/12/2020 09:38 AM - pespin

- Status changed from New to Feedback

I reported the crash together with a link to this same ticket in ofono ML:
https://lists.ofono.org/hyperkitty/list/ofono@ofono.org/thread/IWOBIJL32WCSR2NXPI2HHMM4YC2PEUQ2/

Files

ofono.log	27.2 MB	05/11/2020	pespin