# libosmocore - Bug #2986

## GNU TLS fallback: segfault on gnutls_rnd()

02/22/2018 06:42 PM - fixeria

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Start date:** | 02/22/2018 |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | lynxis | **% Done:** | 100% |
| **Category:** | libosmogsm | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

According to the GNU TLS documentation, prior to 3.3.0 the library has to be initialized by calling gnutls_global_init():

https://www.gnutls.org/manual/html_node/Initialization.html

while the recent versions are being initialized on load. This causes segfault on osmo_get_rand_id() if a library version is lower than 3.3.0...

At the same time, in the configure.am we require gnutls >= 2.12.0.

**Related issues:**

| | | |
|---|---|---|
| Related to OsmoSGSN - Bug #2982: make check: sgsn test failed | **Closed** | **02/22/2018** |
| Related to OsmoMGW - Bug #2981: make check: mgcp test failed | **New** | **02/22/2018** |
| Related to OsmoMSC - Bug #2983: OsmoMSC crashes on LUR | **Closed** | **02/22/2018** |

### History

#### #1 - 02/22/2018 06:42 PM - fixeria

*- Related to Bug #2982: make check: sgsn test failed added*

#### #2 - 02/22/2018 06:43 PM - fixeria

*- Related to Bug #2981: make check: mgcp test failed added*

#### #3 - 02/22/2018 06:43 PM - fixeria

*- Related to Bug #2983: OsmoMSC crashes on LUR added*

#### #4 - 04/10/2018 05:32 PM - laforge

*- Assignee set to lynxis*

#### #5 - 04/10/2018 05:53 PM - fixeria

I have the following suggestions:

- Bump the minimal required version to 3.3.0;
- Initialize the library when libosmocore is loaded (DSO):

```
__attribute__((constructor))
static void on_dso_load_gnutls(void)
{
    gnutls_global_init();
}
```

#### #6 - 04/20/2018 01:21 PM - lynxis

debian/wheezy (old-old-stable): 2.12.20-8+deb7u5
debian/jessie (old-stabe): 3.3.8-6+deb8u
debian/stretch (stable): 3.5.8-5+deb9u3
ubuntu/14.04 LTS: 3.2.11
ubuntu/16.04 LTS: 3.4.10

#### #7 - 04/24/2018 10:15 AM - lynxis

*- Assignee changed from lynxis to laforge*

laforge: can we increase the minimal version to 3.3.0?

#### #8 - 04/24/2018 10:19 AM - lynxis

sysmobts 201705: is using 3.5.9
sysmobts 201310: is using 2.12.23

So we would loose sysmobts 201310 and ubuntu 14.04

#### #9 - 04/24/2018 12:01 PM - lynxis

*- Status changed from New to In Progress*

*- Assignee changed from laforge to lynxis*

#### #10 - 04/24/2018 12:07 PM - laforge

I think we should simply introduce an

```
#if GNUTLS_VERSION < 3.3.0
gnutls_global_init();
#endif
```

I would assume it's pretty straight-forward to do, and not a big burden
in order to gain wider backwards compatibility.

#### #11 - 04/24/2018 02:19 PM - lynxis

I've tried to reproduce this test in a vm with debian wheezy, but it didn't worked out.

```
/* compile with
 * gcc -g -o test_osmo_get_rand_id /tmp/test_osmo_get_rand_id.c -l osmocore -l osmogsm
 */

#include <stdio.h>
#include <stdlib.h>
```

```
#include <osmocom/gsm/gsm_utils.h>

int main() {
    char buffer[16] = { 0 };
    printf("%s\n", osmo_hexdump(buffer, 16));
    int rc = osmo_get_rand_id(buffer, 16);
    printf("%s\n", osmo_hexdump(buffer, 16));
    printf("rc = %d\n", rc);

    exit(0);
}
```

#### #12 - 04/24/2018 02:30 PM - lynxis

*- % Done changed from 0 to 100*

https://gerrit.osmocom.org/#/c/7904/

#### #13 - 04/24/2018 02:31 PM - lynxis

*- Status changed from In Progress to Feedback*

#### #14 - 05/01/2018 04:06 PM - laforge

*- Status changed from Feedback to Stalled*

*- % Done changed from 100 to 90*

#### #15 - 05/02/2018 01:51 PM - lynxis

waiting for review.

#### #16 - 05/03/2018 02:52 AM - lynxis

*- Status changed from Stalled to Resolved*

*- % Done changed from 90 to 100*