OsmoBTS - Bug #4606

osmo-bts-trx: global-buffer-overflow in trx_if_send_burst()

06/09/2020 03:19 PM - pespin

Status: Resolved
Priority: Normal
Assignee: pespin
Category: osmo-bts-trx
Target version: osmo-bts-trx refresh
Spec Reference:

description

I just got this using master osmo-bts with a few more patches (non-related, TRXCM NOMTXPOWER and rump up stuff).
I was testing #4006 and patch https://gerrit.osmocom.org/c/osmo-bts/+/17766 by using "osmotrx fn-advance 2" on phy 0 running a B200 with multi-arfcn enabled (2TRX).

20200609171243003 DTRX <000b> trx_if.c:122 phy0:0: Clock indication: fn=2566102
20200609171243003 DLIC <0006> scheduler_trx.c:1871 TRX Clock Ind: elapsed_us= 997359, elapsed_fn=216, error_us= +519
20200609171243003 DLIC <0006> scheduler_trx.c:1890 GSM clock jitter: -696us (elapsed_fn=0)
20200609171244000 DTRX <000b> trx_if.c:122 phy0:0: Clock indication: fn=2566318
20200609171244000 DLIC <0006> scheduler_trx.c:1871 TRX Clock Ind: elapsed_us= 997798, elapsed_fn=216, error_us= +958
20200609171244000 DLIC <0006> scheduler_trx.c:1890 GSM clock jitter: -1572us (elapsed_fn=0)

==633279==ERROR: AddressSanitizer: global-buffer-overflow on address 0x5555557ff994 at pc 0x7ffff762c2a6 bp 0x7fffffffd7a0 sp 0x7fffffffcf48
READ of size 444 at 0x5555557ff994 thread T0
#0 0x7ffff762c2a5 in __interceptor_memcpy /build/gcc/src/gcc/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:806
#1 0x5555556f11c5 in trx_if_send_burst /home/pespin/dev/sysmocom/git/osmo-bts/src/osmo-bts-trx/trx_if.c:1146
#2 0x55555571d36f in trx_sched_fn /home/pespin/dev/sysmocom/git/osmo-bts/src/osmo-bts-trx/scheduler_trx.c:1661
#3 0x55555571e48a in trx_fn_timer_cb /home/pespin/dev/sysmocom/git/osmo-bts/src/osmo-bts-trx/scheduler_trx.c:1758
#4 0x7ffff683af76 in osmo_fd_disp_fds /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:27
#5 0x7ffff683b35b in __osmo_select_main /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:265
#6 0x7ffff683b43a in __osmo_select_main /home/pespin/dev/sysmocom/git/libosmocore/src/select.c:274
#7 0x5555557c8306 in bts_main /home/pespin/dev/sysmocom/git/osmo-bts/src/common/main.c:354
#8 0x5555555e5027 in main /home/pespin/dev/sysmocom/git/osmo-bts/src/osmo-bts-trx/main.c:159
#9 0x7ffff5bf4001 in __libc_start_main (/usr/lib/libc.so.6+0x27001)
#10 0x55555556e41fd in __start (/home/pespin/dev/sysmocom/build/new/out/bin/osmo-bts-trx+0x1901f)

0x5555557ff994 is located 0 bytes to the right of global variable 'dummy_burst' defined in '/home/pespin/dev/sysmocom/git/osmo-bts/src/common/scheduler.c:53:21' (0x5555557ff900) of size 148
0x5555557ff994 is located 44 bytes to the left of global variable '_sched_fcch_burst' defined in '/home/pespin/dev/sysmocom/git/osmo-bts/src/common/scheduler.c:64:14' (0x5555555ff9c0) of size 148
Shadow bytes around the buggy address:
0x0aabb2aaf7ee0: f0 f9 f9 f9 00 00 00 00 00 00 00 00 00 00 00 00
0x0aabb2aaf7ef0: 00 03 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
0x0aabb2aaf7f00: 04 f9 f9 f9 f9 f9 f9 f9 f9 00 00 00 00 00 00 00 00
0x0aabb2aaf7f10: 00 02 f9 f9 f9 f9 f9 f9 00 00 00 07 f9 f9 f9 f9
0x0aabb2aaf7f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0aabb2aaf7f30: 00 [04]f9 f9 f9 f9 00 00 00 00 00 00 00 04 f9 f9 f9 f9
0x0aabb2aaf7f40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0aabb2aaf7f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

08/08/2021
Program received signal SIGABRT, Aborted.

--Type <RET> for more, q to quit, c to continue without paging--
0x00007fffffff5c09355 in raise () from /usr/lib/libc.so.6

(gdb)

Associated revisions
Revision 0bf87ccc - 06/12/2020 10:01 AM - pespin
scheduler: Fix reading out of buffer during tx of dummy burst on PDCH TS with EGPRS enabled

If for whatever reason (eg fn-advance too small) there's no burst available for a PDCH TS where EGPRS is enabled, a dummy burst of size GSM_BURST_LEN would be selected in _sched_dl_burst(), but the nbits length would still be set to EGPRS_BURST_LEN above by func() pointer (tx_pdtch_fn()). As a result, trx_if_send_burst() would later read EGPRS_BURST_LEN from the dummy burst of size GSM_BURST_LEN.

The issue was found by ASan. See OS#4606 for more info.

Fixes: OS#4606
Change-Id: Iba6ccceed5c0f1db810259768678f174d39cb8b

History
#1 - 06/09/2020 03:24 PM - pespin

(gdb) bt
# 0 0x00007fffffff5c09355 in raise () from /usr/lib/libc.so.6
# 1 0x00007fffffff5b2853 in abort () from /usr/lib/libc.so.6
# 2 0x00007fffffff76c2a34 in __sanitizer::Abort () at /build/gcc/src/gcc/libsanitizer/sanitizer_common/sanitizer_posix_libcdep.cpp:155
# 3 0x00007fffffff76ce53d in __sanitizer::Die () at /build/gcc/src/gcc/libsanitizer/sanitizer_common/sanitizer_termination.cpp:58
# 4 0x00007fffffff76ad222 in __asan::ScopedInErrorReport::__ScopedInErrorReport () at /build/gcc/src/gcc/libasanitizer/sanitizer_common/sanitizer_termination.cpp:58
# 5 0x00007fffffff76ad53d in __asan::ScopeInErrorReport () at /build/gcc/src/gcc/libasanitizer/sanitizer_common/sanitizer_termination.cpp:58
# 6 0x00007fffffff76ad53d in __asan::ScopeInErrorReport () at /build/gcc/src/gcc/libasanitizer/sanitizer_common/sanitizer_termination.cpp:58
# 7 0x00007fffffff76ad53d in __asan::ScopeInErrorReport () at /build/gcc/src/gcc/libasanitizer/sanitizer_common/sanitizer_termination.cpp:58

08/08/2021
It seems global buffer dummy_burst (static const ubit_t dummy_burst[GSM_BURST_LEN] = { }) of size GSM_BURST_LEN=148 is being passed but since I'm using EGPRS, one of EGPRS_BURST_LEN=444 should be passed.

#2 - 06/09/2020 03:45 PM - pespin

It seems TS 05.02 chapter 5.2.6 only defines bursts for GMSK afaiu

https://www.etsi.org/deliver/etsi_ts/100900_100999/100908/08.11.00_60/ts_100908v081100p.pdf

We could do this to fix the issue once find out which kind of burst we need to send there:

diff --git a/src/common/scheduler.c b/src/common/scheduler.c
index 55cb36a7..f22f2eb4f 100644
--- a/src/common/scheduler.c
+++ b/src/common/scheduler.c
@@ -1210,7 +1210,13 @@ no_data:
     "burst=%d on C0, so filling with dummy burst\n",
    trx_chan_desc[chan].name, fn, tn, bid);
 #endif
-     bits = (ubit_t *) dummy_burst;
+     if (nbits == GSM_BURST_LEN)
+        bits = (ubit_t *) dummy_burst;
+     else if (nbits == EGPRS_BURST_LEN)
+        bits = (ubit_t *) egprs_dummy_burst;
+     else
+        osmo_panic("%s:%d Requested dummy burst for invalid burst len %d\n",
+                     __FILE__, __LINE__, nbits);
+     }

     return bits;

#3 - 06/09/2020 04:06 PM - pespin

- Status changed from New to Feedback
- % Done changed from 0 to 90

I finally simply set nbits to the correct buffer size.

Should be fixed by:
remote: https://gerrit.osmocom.org/c/osmo-bts/+18750 scheduler.c: Fix trailing whitespace
remote: https://gerrit.osmocom.org/c/osmo-bts/+18751 scheduler: Fix reading out of buffer during tx of dummy burst on PDCH TS ...

#4 - 06/25/2020 05:05 PM - pespin

- Status changed from Feedback to Resolved
- % Done changed from 90 to 100

Merged, closing.