**Freeciv - Bug #858251**

**SEGv in name_translation_get (2.6.1+, qt)**

2020-02-03 02:49 AM - Chippo Elder

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Marko Lindqvist</td>
</tr>
<tr>
<td>Category:</td>
<td>gui-qt</td>
</tr>
<tr>
<td>Sprint/Milestone:</td>
<td>2.6.2.1</td>
</tr>
</tbody>
</table>

**Description**

I was trying to trigger [858212](#858212) (you can see all the tileset loads in the transcript) without success. I decided to try something in the gtk client while in a Start Game screen and I hit Disconnect. Got the following dump-thingy:

```bash
chippo@chippo-Aspire-V3-731:~$ ASAN_OPTIONS="abort_on_error=1:disable_coredump=0:unmap_shadow_on_exit=1" freeciv-qt-26
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
QSocketNotifier: Invalid socket 41 and type 'Read', disabling...
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "amplio2".
2: Loading tileset "amplio_earth".
libpng warning: iCCP: known incorrect sRGB profile
libpng warning: iCCP: known incorrect sRGB profile
libpng warning: iCCP: known incorrect sRGB profile
libpng warning: iCCP: known incorrect sRGB profile
QSocketNotifier: Invalid socket 41 and type 'Read', disabling...
qt.qpa.xcb: QXcbConnection: XCB error: 3 (BadWindow), sequence: 15998, resource id: 18906179, major code: 40
(TranslateCoords), minor code: 0
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "trident".
2: Loading tileset "amplio2".
QSocketNotifier: Invalid socket 41 and type 'Read', disabling...
2: last message repeated 2 times
AddressSanitizer:DEADLYSIGNAL
```

```
=================================================================
==256157==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000078 (pc 0x00000082e0d4 bp 0x7ffc9e059090 sp 0x7ffc9e059090 T0)
==256157==The signal is caused by a READ memory access.
@==256157==Hint: address points to the zero page.
#0 0x82e0d3 in name_translation_get /home/chippo/Downloads/git_clones/freeciv/common./name_translation.h:123:18
#1 0x82deec in nation_plural_translation /home/chippo/Downloads/git_clones/freeciv/common/nation.c:161:10
#2 0x82e140 in nation_plural_for_player /home/chippo/Downloads/git_clones/freeciv/common/nation.c:179:10
#3 0x539211 in show_new_turn_info() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#4 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#5 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#6 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#7 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#8 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#9 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#10 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#11 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#12 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#13 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#14 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#15 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#16 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
#17 0x555682e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/hudwidget.cpp:1664:19
```

2021-08-22

1/4
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/chippo/Downloads/git_clones/freeciv/common/./name_translation.h:123:18 in name_translation_get
@==256157==ABORTING
Aborted (core dumped)

And GDB's contribution:
Core was generated by `freeciv-qt-26`.
Program terminated with signal SIGABRT, Aborted.
#0  _GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50 ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
[Current thread is 1 (Thread 0x00007fcfeedar6ac0 (LWP 256157))]
(gdb) bt full
#0  _GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
set = {__val = {0, 5106555, 895, 0, 0, 281470681751424, 0, 0, 0, 0, 0, 0, 0, 0, 0}}
pid = <optimized out>
tid = <optimized out>
#1 0x00007fcc3e6899 in _GI_abort () at abort.c:79
save_stage = 1
act = (__sigaction_handler = {sa_handler = 0x0, sa_sighandler = 0x0}, sa_mask = {__val = {0, 1024, 5187702, 13733576, 140531153141536, 2, 0, 0, 0, 0, 0, 3, 0, 0}}, sa_flags = 0, sa_restorer = 0x86a68 __asan::error_message_buf_mutex>)
sigs = (__val = {32, 0 <repeats 15 times>})
#2 0x00000000004f8e27 in ()
#3 0x00000000004f7801 in ()
#4 0x00000000004f389 in ()
#5 0x00000000004f0f13 in _asan::ReportDeadlySignal(_sanitizer::SignalContext const&) ()
#6 0x00000000004f9e9c in __asan::AsanOnDeadlySignal(int, void*, void*) ()
#7 0x00007fcc3e44540 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
**Related issues:**
Related to Freeciv - Bug #857974: Qt client with -t augmented dumps core (2.6.1+) added

**History**

#1 - 2020-02-10 11:40 PM - Jacob Nevins

This is the same signature cazfi notes in #857974-1, so it's probably related.

#2 - 2020-02-10 11:40 PM - Jacob Nevins
- Related to Bug #857974: Qt client with -t augmented dumps core (2.6.1+) added

#3 - 2020-04-22 12:33 PM - Marko Lindqvist
- Category set to gui-qt
- Status changed from New to In Progress
- Sprint/Milestone set to 2.6.3

#4 - 2020-04-25 08:22 PM - Marko Lindqvist
- Status changed from In Progress to Closed
- Assignee set to Marko Lindqvist

Jacob Nevins wrote:

This is the same signature cazfi notes in #857974-1, so it's probably related.

Fixed in Bug #857974

#5 - 2020-11-16 02:10 AM - Marko Lindqvist
- Sprint/Milestone changed from 2.6.3 to 2.6.2.1