I ran 'freeciv-qt -t augmentedi'. I was starting games with random rulesets and random changes to Game options, and if the game started ok, then quit and try again. I was looking for trouble (like a core dump), found it, then got confused with my own note-taking and can't reproduce it, or be sure what I did when it triggered.

Core was generated by 'freeciv-qt'. Program terminated with signal SIGSEGV, Segmentation fault.
#24 0x00000563b00445ee1 in fc_client::fc_main(QApplication*) (this=0x563b017f8270, qapp=0x563b0143c120) at fc_client.cpp:257
#25 0x00000563b003226d3 in qtg_ui_main(int, char**) (argc=1, argv=0x7fff82e71708) at client_main.c:685
i = 1
loglevel = LOG_NORMAL
ui_options = <optimized out>
option = <optimized out>
fatal_assertions = -1
--Type <RET> for more, q to quit, c to continue without paging--c
aii = 1
FUNCTION = "client_main"
#27 0x000005631ea9fa163 in __libc_start_main (main=0x563b00320460 <main(int, char**)>, argc=1, argv=0x7fff82e71708, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fff82e716f8) at ../csu/libc-start.c:308
result = <optimized out>
not_first_call = <optimized out>

#28 0x00000563b003217ae in _start () at gui_main.cpp:114

Related issues:
- Related to Freeciv - Bug #857869: Qt SEGV in Cancel of Load Game (2.6.1+) Closed
- Related to Freeciv - Bug #858251: SEGv in name_translation_get (2.6.1+, qt) Closed

History
#1 - 2020-01-30 04:31 PM - Marko Lindqvist
Chippo Elder wrote:

This call-chain is showing up in several of your backtraces in different tickets. I think qt_start_turn() gets called when client state is not suitable for it. I
don't know why Qt-client has that qt_start_turn() call in qtg_update_timeout_label(). Other clients do not have equivalent call in their
update_timeout_label() function.

Marko Lindqvist wrote:

I considered patching over that design in S2_6, but it turned out that there's no low-impact way to do it, so I'm going to full clean gui API change even in
S2_6. As qt_start_turn() call goes away from qtg_update_timeout_label(), any ticket with backtrace with that call chain should be closed if my patch
gets accepted.

#2 - 2020-02-01 01:01 PM - Jacob Nevins
- Related to Bug #857869: Qt SEGV in Cancel of Load Game (2.6.1+) added

#3 - 2020-02-10 11:40 PM - Jacob Nevins
- Related to Bug #858251: SEGv in name_translation_get (2.6.1+, qt) added

#4 - 2020-04-22 01:00 PM - Marko Lindqvist
- Category set to Client
- Status changed from New to In Progress
- Sprint/Milestone set to 2.6.3

Marko Lindqvist wrote:

I don't know why Qt-client has that qt_start_turn() call in qtg_update_timeout_label(). Other clients do not have equivalent call in their
update_timeout_label() function.

#5 - 2020-04-22 02:15 PM - Marko Lindqvist
- File 0022-Fix-Qt-client-crash-on-timeout-label-update.patch added
- File 0010-Fix-Qt-client-crash-on-timeout-label-update.patch added
- File 0006-Fix-Qt-client-crash-on-timeout-label-update.patch added
- Status changed from In Progress to Resolved

Patches that reimplement affected code. In any case this is cleaner implementation. I believe it to also avoid the crashes of the old implementation.

#6 - 2020-04-25 08:20 PM - Marko Lindqvist
- Status changed from Resolved to Closed
- Assignee set to Marko Lindqvist

#7 - 2020-11-16 02:10 AM - Marko Lindqvist
- Sprint/Milestone changed from 2.6.3 to 2.6.2.1

Files

<table>
<thead>
<tr>
<th>Patch Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0022-Fix-Qt-client-crash-on-timeout-label-update.patch</td>
<td>10.9 KB</td>
<td>2020-04-22</td>
<td>Marko Lindqvist</td>
</tr>
<tr>
<td>0010-Fix-Qt-client-crash-on-timeout-label-update.patch</td>
<td>11.3 KB</td>
<td>2020-04-22</td>
<td>Marko Lindqvist</td>
</tr>
<tr>
<td>0006-Fix-Qt-client-crash-on-timeout-label-update.patch</td>
<td>13.4 KB</td>
<td>2020-04-22</td>
<td>Marko Lindqvist</td>
</tr>
</tbody>
</table>