Description
I was trying to trigger #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:

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".
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 0x556582e in qt_start_turn() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/menu.cpp:78:3
#5 0x555042e in qtg_update_timeout_label() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/mapview.cpp:1086:5
#6 0x5550d7f in update_timeout_label /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/mapview.cpp:1086:5
#7 0x5de37f7 in stop_turn_change_wait /home/chippo/Downloads/git_clones/freeciv/client/client_main.cpp:1131:3
#8 0x6030c2 in disconnect_from_server /home/chippo/Downloads/git_clones/freeciv/client/client_main.cpp:1131:3
#9 0x7435cf in fc_client::slot_disconnect() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/fc_client.cpp:497:5
#10 0x556566e in QPrivate:::FunctorCall<QPrivate::IndexesList<>, QtPrivate::List<> void, void (fc_client::*())>::call(void (fc_client::*()), fc_client*, void*) /usr/include/x86_64-linux-gnu/qt5/QtCore/Qobjectdefs_impl.h:152:13
#11 0x555d48e in void QPrivate:::FunctionPointer< void (fc_client::*())>::call(QPrivate::List<> void*, void (fc_client::*()), fc_client*, void*) /usr/include/x86_64-linux-gnu/qt5/QtCore/Qobjectdefs_impl.h:185:13
#12 0x5553a7 in QPrivate:::SlotObject< void (fc_client::*()) QPrivate::List<> void> impl(int, QPrivate::QSLOTObjectBase*, QObject*, void**, bool*) /usr/include/x86_64-linux-gnu/qt5/QtCore/Qobjectdefs_impl.h:414:17
#13 0x7fffe48bc5c7 in QMetaObject::activate(QObject*, int, int, void**) /usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x215c7
#14 0x7fffe41a1235 in QAbstractButton::clicked(bool) /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x2f235
#15 0x7fffe41a145d /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x2f235d
#16 0x7fffe41a28a2 /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x2608a2
#17 0x7fffe41a2a64 in QAbstractButton::mouseReleaseEvent(QMouseEvent*)
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 augmentedi 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