Freeciv - Bug #863815

SEGV on unknown address in player_has_real_embassy (S3_0)

2020-03-08 11:00 AM - Chippo Elder

Status: Closed
Priority: Normal
Assignee: Marko Lindqvist
Category: gui-qt
Sprint/Milestone: 2.6.2.1

Start date: 
Due date: 
% Done: 0%
Estimated time: 0.00 hour

Description

I was running a separate server and client (qt) and I quit the server with a 'quit' command and got the following dump in the client:

chippo@chippo-Aspire-V3-731:~/Downloads/git_clones/freeciv/freeciv-30$ ASAN_OPTIONS="abort_on_error=1:disable_coredump=0:unmap_shadow_on_exit=1:detect_leaks=0" ./fcgui --gui qt

Running ./client/freeciv-qt

2: Loading tileset "hexemplio".

AddressSanitizer:DEADLYSIGNAL

=================================================================
==1931591==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000e1 (pc 0x000000916834 bp 0 x7fffbab81c80 sp 0x7fffbab81c60 T0)
==1931591==The signal is caused by a READ memory access.
==1931591==Hint: address points to the zero page.
#0 0x916833 in player_has_real_embassy /home/chippo/Downloads/git_clones/freeciv/freeciv-30/common/player.c:214:10
#1 0x9167cc in player_has_embassy /home/chippo/Downloads/git_clones/freeciv/freeciv-30/common/player.c:203:14
#2 0x729b8f in plr_widget::nation_selected(QItemSelection const&, QItemSelection const&) /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/plrdlg.cpp:454:11
#3 0x7962f4 in plr_widget::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/meta_plrdlg.cpp:313:21
#4 0x7fb3f5a753f7 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x2b13f7)
#5 0x7fb3f5a050c3 in QItemSelectionModel::selectionChanged(QItemSelection const&, QItemSelection const&) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x2410c3)
#6 0x7fb3f5a07531 in QItemSelectionModel::setCurrentIndex(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243531)
#7 0x7fb3f5a07300 in QItemSelectionModel::setCurrentIndex(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243300)
#8 0x7fb3f5a07531 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243531)
#9 0x7fb3f5a07300 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243300)
#10 0x7fb3f54fca2c in QAbstractItemView::setCurrentIndex(QModelIndex const&) (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x3d1a2c)
#11 0x72d5f0 in plr_report::update_report(bool) /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/plrdlg.cpp:822:16
#12 0x7b7000 in real_players_dialog_update /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/plrdlg.cpp:911:11
#13 0x5d332c in update_unqueue /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/update_queue.c:320:15
#14 0x6a86d in mr_idle::idling() /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/mapview.cpp:175:5
#15 0x6b88c6 in QPrivate::FunctorCall<QPrivate::IndexesList<> QPrivate::List<> void, void (mr_idle::*())>::call(void (mr_idle::*())(), mr_idle*, void**) /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:152:13
#16 0x6b87a8 in QPrivate::FunctionPointer<void (mr_idle::*())>::call(QPrivate::List<>, void) (mr_idle::*())() /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:185:13
#17 0x6b8707 in QPrivate::QSlotObject<void (mr_idle::*())(), QPrivate::List<> void>::impl(int_, QPrivate::QSlotObjectBase*, QObject*, void**, bool) /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:141:17
#18 0x7fb3f5a75557 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x2b13f7)
#12 0x00007fb3f35a753f8 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#13 0x00007fb3f35a050c4 in QItemSelectionModel::selectionChanged(QItemSelection const&, QItemSelection const&) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#14 0x00007fb3f35a050d0 in QItemSelectionModel::emitSelectionChanged(QItemSelection const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#15 0x00007fb3f35a05dd0 in QItemSelectionModel::select(QItemSelection const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#16 0x00007fb3f35a07301 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#17 0x00007fb3f5a07532 in QItemSelectionModel::setCurrentIndex(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#18 0x000000000070a4a0 in QAbstractItemView::setSelection(QModelIndex const&, QFlags<QAbstractItemView::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#19 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#20 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#21 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#22 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#23 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#24 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#25 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#26 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#27 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#28 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#29 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#30 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#31 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#32 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#33 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#34 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#35 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#36 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#37 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#38 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#39 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#40 0x000000000070a4a0 in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5

2021-08-06
I can't replicate it.

History

#1 - 2020-04-22 09:47 AM - Marko Lindqvist
- Tracker changed from Task to Bug
- Status changed from New to In Progress
- Sprint/Milestone set to 2.6.3

Like backtraces in several other tickets, this shows

mr_idle::idling()

after the client is supposedly left the game. It tries to execute callbacks registered while the game was still running, and which try to update widgets like it still was in a game.

#2 - 2020-04-22 10:44 AM - Marko Lindqvist

Marko Lindqvist wrote:

... backtraces in several other tickets ...

Unfortunately there's no easy way to implement "catch all" solution. It seems we need to make necessary checks, per ticket, inside the running callbacks.

#3 - 2020-04-22 11:06 AM - Marko Lindqvist

Did you happen to be global observer at the time? For this crash to happen client can't be attached to a player. That can happen at least when one is global observer. I'm not sure if it can happen because client is already leaving the game (if you weren't global observer, it would be the only explanation).

The crash also required player with no research selected to be selected in the player dialog. The fact that crash happens just when client is leaving the game is probably explained by removal of the other players from the player dialog. When previously selected player is removed, new one gets to be the selected one, and eventually that hits player that has no research selected.

#4 - 2020-04-22 11:14 AM - Marko Lindqvist
- File 0009-Qt-Fix-plrdialog-crash-when-selected-player-has-no-r.patch added
- Status changed from In Progress to Resolved

Attached patch should fix at least the crash seen in the backtrace. There's no guarantees it doesn't still crash later in the codepath.

#5 - 2020-04-26 07:14 PM - Marko Lindqvist
- Status changed from Resolved to Closed
- Assignee set to Marko Lindqvist

#6 - 2020-11-16 02:11 AM - Marko Lindqvist
- Sprint/Milestone changed from 2.6.3 to 2.6.2.1