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_erro
r=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 0x916833 bp 0
x7ffbab81c80 sp 0x7ffbab81c60 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/co
mmon/player.c:214:10
#1 0x9167cc in player_has_embassy /home/chippo/Downloads/git_clones/freeciv/freeciv-30/com
mon/player.c:203:14
#2 0x729b8f in plr_widget::nation_selected(QItemSelection const&, QItemSelection const&) /home/cl
inho/Downloads/git_clones/freeciv/freeciv-30/client/gui-qt/plrdlg.cpp:454:11
#3 0x7962f4 in QItemSelectionModel::emitSelectionChanged(QItemSelection const&, QItemSelection M
odel::SelectionFlag) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x2410c3)
#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
Model::SelectionFlag) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x246501)
#6 0x7fb3f35a050d6 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionM
odel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243531)
#7 0x7fb3f35a050c3 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionM
odel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243300)
#8 0x7fb3f35a07300 in QItemSelectionModel::selectCurrentIndex(QModelIndex const&, QFlags<QItemSelectionM
odel::SelectionFlag>) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x243531)
#9 0x7fb3f35a07351 in QAbstractItemView::setCurrentIndex(QModelIndex const&) (/usr/lib/x86_64-
linux-gnu/libQt5Widgets.so.5+0x3d1a2c)
#10 0x7fb3f354fca2c 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 0x730700 in update_unqueue /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/upd
ate_queue.c:320:15
#13 0x5d332c in update_queue /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/upd
ate_queue.c:320:15
#14 0x6a86d in mr_idle::idling() /home/chippo/Downloads/git_clones/freeciv/freeciv-30/client/u
pdate_queue.c:320:15
#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/Q
Core/qobjectdefs_impl.h:152:13
#16 0x6b87e8 in void QPrivate::FunctionPointer<void (mr_idle::*)(*):::call(QPrivate::List<>*,
void) (mr_idle::*)(*), mr_idle*, void**)) /usr/include/x86_64-linux-gnu/qt5/QPrivate/qobjec
tdefs_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/QPrivate/q
objectdefs_impl.h:141:17
#18 0x7fb3f5a75557 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux
```
AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/chippo/Downloads/git_clones/freeciv/freeciv-30/common/player.c:214:10 in player_has_real_embassy

Aborted (core dumped)

BT:

Core was generated by `/client/freeciv-qt'.
Program terminated with signal SIGABRT, Aborted.
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
     ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
[Current thread is 1 (Thread 0x7fb3f18a7b80 (LWP 1931591))]
(gdb) bt full
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
     set =
     (_val = {0, 5112187, 140410958843328, 140410958843328, 140410958843328, 5201184, 206158430216, 1404109588433968, 1404109588433776, 5198849, 0, 13535464, 140736326017024, 23545844, 206158430216, 1404109588433968})
     pid = <optimized out>
     tid = <optimized out>
#1  0x000007f3f34c442899 in __GI_abort () at abort.c:79
     save_stage = 1
     act =
     (__sigaction_handler = (sa_handler = 0x7fb3f94ef000, sa_sigaction = 0x7fb3f94ef000), sa_mask = {__val = {0, 4096, 1024, 5193334, 14134600, 140410958843680, 2, 0, 0, 0, 0, 0, 0, 140737488355327, 5193334, 80}), sa_flags = 5199443, sa_restorer = 0xce88e8 <__asan::error_message_buf_mutex
sigs = {__val = {32, 0 <repeats 15 times>}}

#2 0x0000000000004fa427 in ()
#3 0x0000000000004f8e01 in ()
#4 0x0000000000004e0989 in ()
#5 0x0000000000004e06e13 in __asan::ReportDeadlySignal(__sanitizer::SignalContext const&) ()
#6 0x0000000000004d4f3c in __asan::SanonDeadlySignal(int, void*, void*) ()
#7 0x000007f3f51d540 in <signal handler called> () at /lib/x86_64-linux-gnu/libpthread.so.0
#8 0x00000000000916834 in player_has_real_embassy (pplayer=0x0, pplayer2=0x61e000020480) at player.c:21
#9 0x000000000009167cd in player_has_embassy (pplayer=0x0, pplayer2=0x61e000020480) at player.c:20
#10 0x00000000000729b90 in plr_widget::nation_selected(QItemSelection const&, QItemSelection const&) at plrdlg.cpp:454

entry_exist = false
pplayer = 0x61e000020480
me = 0x0
research = 0x16747f4 <research_array+97812>
pcity = <optimized out>
added = <optimized out>
state = <optimized out>
tech_id = <optimized out>
a = <optimized out>
b = <optimized out>
my_research = <optimized out>

res = {static null = {<No data fields>}, d = 0x7fb3f5b2a680 <QArrayData::shared_null>}
sp = {static null = {<No data fields>}, d = 0x6030000d00f0}
est = {static null = {<No data fields>}, d = 0x7fb3f5b2a680 <QArrayData::shared_null>}
esci = {static null = {<No data fields>}, d = 0x7fb3f5b2a680 <QArrayData::shared_null>}
elux = {static null = {<No data fields>}, d = 0x7fb3f5b2a680 <QArrayData::shared_null>}
egold = {static null = {<No data fields>}, d = 0x7fb3f5b2a680 <QArrayData::shared_null>}
egov = <optimized out>
cult = <optimized out>
nl = <optimized out>
sorted_list_a = {<QList<QString>> = {<QListSpecialMethods<QString>> = {<No data fields>},
(p = {static shared_num = {atomic = <std::atomic_base<int>> = {static _alignment = 4, _M_i = -1},
<No data fields>}}), alloc = 0, begin = 0, end = 0, array = (0x0)}, d = 0x6110006c2900}, d = 0x6110006c2900}
sorted_list_b = {<QList<QString>> = {<QListSpecialMethods<QString>> = {<No data fields>},
(p = {static shared_num = {atomic = <std::atomic_base<int>> = {static _alignment = 4, _M_i = -1},
<No data fields>}}), alloc = 0, begin = 0, end = 0, array = (0x0)}, d = 0x7fb3f5b2c760 <QListData::shared_null>}, d = 0x7fb3f5b2c760 <QListData::shared_null>}, <No data fields>}}
entry_exist = false
pplayer = 0x61e000020480
me = 0x0
research = 0x16747f4 <research_array+97812>
pcity = <optimized out>
added = <optimized out>
state = <optimized out>
tech_id = <optimized out>
a = <optimized out>
b = <optimized out>
my_research = <optimized out>

11 0x00000000000729b90 in plr_widget::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) (_o=0xel, _c=<optimized out>, _id=<optimized out>, _a=0x1) at meta_plrdlg.cpp:313
_t = 0xel

2021-08-08 3/6
#12 0x00007fb3f5a753f8 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#13 0x00007fb3f5a050c4 in QItemSelectionModel::selectionChanged(QItemSelection const&, QItemSelection const&) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#14 0x00007fb3f5a05a502 in QItemSelectionModel::emitSelectionChanged(QItemSelection const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#15 0x00007fb3f5a0d0d7 in QItemSelectionModel::select(QModelIndex const&, QFlags<QItemSelectionModel::SelectionFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#16 0x00007fb3f5a07301 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/libQt5Core.so.5
#18 0x00007fb3f5a07f54ca2d in QAbstractItemView::setCurrentIndex(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#19 0x00000000000702d5f1 in plr_report::update_report(bool) (this=<optimized out>, update_selection=<optimized out>) at plrdlg.cpp:822
qmi = {r = 9, c = 0, i = 105828001898704, m = 0x6020002ad9f0}
player_count = 0
#20 0x000000000007030701 in real_players_dialog_update(void*) (unused=<optimized out>) at plrdlg.cpp:911
i = 3
pr = 0x0
w = 0x0
#21 0x000000000007030703 in update_unqueue (data=<optimized out>) at update_queue.c:320
callback = 0x7305a0 <real_players_dialog_update(void*)>
uq_data = 0x0
__vla_expr0 = <optimized out>
MY_mem_MY_iter = <optimized out>
MY_it_MY_iter = 0x7fffbab841c0
MY_iter = 0x7fffbab841c0
hash = 0x607000366f60
#22 0x000000000006ad86e in mr_idle::idling() (this=<optimized out>) at mapview.cpp:175
cb = 0x6020002790f0
#23 0x000000000006b8b7c in QtPrivate::FunctorCall<QtPrivate::IndexesList, QtPrivate::List, void, void, QtPrivate::List>(::call(void (mr_idle::*())(mr_idde, void**, void**) {f=<optimized out>, o=<optimized out>, arg=<optimized out>) at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:152
#24 0x000000000006b8be9 in QtPrivate::FunctionPointer<void (mr_idle::*())(mr_idde, void*, void**) {f=virtual table offset 224, this adjustment 10761470070800, o=0xc, arg=0x1} at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:185
#25 0x000000000007068b70 in QtPrivate::QObjectPrivate::notify_helper(QObject*, QEvent*) () at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:185
#26 0x000000000006ad86e in mr_idle::idling() (this=<optimized out>) at mapview.cpp:175
impl(int, QtPrivate::QSlotObjectBase*, QObject*, void**, bool*) (which=<optimized out>, this_=0x603000d9e40, r=0xc, a=0x1, ret=0x604000147920) at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:414
#27 0x000000000006b8bb in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#28 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#29 0x000000000006b8b7e9 in QtPrivate::FunctionPointer<void (mr_idle::*())(mr_idde, void*, void**) {f=virtual table offset 224, this adjustment 10761470070800, o=0xc, arg=0x1} at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:185
#30 0x000000000007068b70 in QtPrivate::QObjectPrivate::notify_helper(QObject*, QEvent*) () at /usr/include/x86_64-linux-gnu/qt5/QtCore/qobjectdefs_impl.h:185
#31 0x000000000006b8bb in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#32 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#33 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#34 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#35 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#36 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#37 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#38 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#39 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#40 0x000000000006b8b25b in QTimer::timeout(Qtimer::QPrivateSignal) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
2021-08-08
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

mrIdle::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
<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0009-Qt-Fix-plrdialog-crash-when-selected-player-has-no-r.patch</td>
<td>1.2 KB</td>
<td>2020-04-22</td>
<td>Marko Lindqvist</td>
</tr>
</tbody>
</table>