Freeceiv - Bug #854917

in get_building_bonus() [effects.c::804]: assertion '((void *)0) != pcity && ((void *)0) != building' failed

2020-01-06 08:54 PM - Chippo Elder

Status: Closed
Priority: Normal
Assignee: Marko Lindqvist
Category: gui-qt
Sprint/Milestone: 3.1.0

Description
I did a git clone, make and got this version:
This is Freeciv version 3.0.91-dev, gui-gtk-3.22 client.
Built against gtk+ 3.24.12, using 3.24.12
Built against glib 2.62.1, using 2.62.1

Some 15 minutes into a new civ2civ3 game I looked at the console and saw:

1: in get_building_bonus() [effects.c::804]: assertion '((void *)0) != pcity && ((void *)0) != building' failed.
1: Please report this message at https://www.hostedredmine.com/projects/freeciv
1: in get_building_bonus() [effects.c::804]: assertion '((void *)0) != pcity && ((void *)0) != building' failed.
1: Please report this message at https://www.hostedredmine.com/projects/freeciv

I don't know what else to add. Let me know if I can send in anything useful. The actual game seems to be behaving as expected.

Related issues:
Has duplicate Freeciv - Bug #860058: SEGV on unknown address (master, qt) Closed

History
#1 - 2020-02-06 01:57 PM - Chippo Elder
I got this in master, 3.0.92-dev (modified 5fa96c064c).

chippo@chippo-Aspire-V3-731:~$ ASAN_OPTIONS="abort_on_error=1:disable_coredump=0:unmap_shadow_on_exit=1:detect_leaks=0" freeciv-qt-dev -F
3: Loading tileset "hexemplio".
3: Loading tileset "amplio2".
0: in get_building_bonus() [effects.c::804]: assertion '((void*)0) != pcity && ((void*)0) != building' failed.
0: Please report this message at https://www.hostedredmine.com/projects/freeciv
Aborted (core dumped)

But this time I've got a core.

Core was generated by `freeciv-qt-dev -F'.
Program terminated with signal SIGABRT, Aborted.
#0  raise (sig=<optimized out>) 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 0x7faac8716080 (LWP 598908))]
(gdb) bt full
#0  raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
0x0000000000000000 in fc_assert_fail
(file=<optimized out>, function=<optimized out>, line=<optimized out>, assertion=<optimized out>, message=2022-08-26
#2 0x000000000083ce4c in get_building_bonus (pcity=0x0, building=<optimized out>, effect_type=<optimized out>) at effects.c:804
#3 0x000000000084fe7e in impr_build_shield_cost (pcity=0x2, pimprove=0x7ffe5280b380) at improvement.c:253
#4 0x00000000005ea1a6 in get_tooltip_improvement (impr_type*, city*, bool) (building=<optimized out>, pcity=<optimized out>, ext=<optimized out>) at citydlg.cpp:3793
upkeep = {static null = {<No data fields>}, d = 0x603000784bd0}
s1 = {static null = {<No data fields>}, d = 0x7faaccc7d680}<QArrayData::shared_null>
s2 = {static null = {<No data fields>}, d = 0x604000d73550}
str = {static null = {<No data fields>}, d = 0x61100010e9a00}
def_str = {static null = {<No data fields>}, d = 0x61100010e9a00}
req = <optimized out>
#5 0x0000000000741bcc in research_diagram::mouseMoveEvent(QMouseEvent*) (this=<optimized out>) at repodlgs.cpp:779
...buf2 = ""
tt_text = {static null = {<No data fields>}, d = 0x7faaccc7d680}<QArrayData::shared_null>
i = 26
ttp = 0x504000007c990
#6 0x00007faacc42b04e in QWidget::event(QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#7 0x00007faacc3e8a86 in QApplicationPrivate::notify_helper(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#8 0x00007faaccf84d73 in QGuiApplicationPrivate::processMouseEvent(QWindowSystemInterfacePrivate::MouseEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Gui.so.5
#9 0x00007faaccf865fb in QWindowSystemInterface::sendWindowSystemEvents(QFlags<QEventLoop::ProcessEventsFlag>) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#10 0x00007faaccba33a6 in fc_client::fc_main(QApplication*) (this=<optimized out>, qapp=<optimized out>) at fc_client.cpp:257
#11 0x000000000050d9ba in ui_main (argc=2, argv=0x7ffe5280b380) at gui_interface.c:59
#12 0x0000000000512628 in client_main (argc=1, argv=<optimized out>) at client_main.c:685
loglevel = <optimized out>
fatal_assertions = <optimized out>
option = <optimized out>
ui_separator = <optimized out>
ui_options = 0
i = <optimized out>
aii = <optimized out>
#30 0x000000000050d3eb in main(int, char**) (argc=2, argv=0x7ffe5280b380) at gui_main.cpp:100
Since I've had this bug in both gtk and qt clients, you'd think that it is a server-side crash. But no! I restarted the client (to grab it's version info) and it plonks me back into the running game.

I think I'm always going to run the server by hand in future. It sure makes it easier to be sure where the crash was.

#2 - 2020-04-16 07:00 AM - Marko Lindqvist
That Qt-client backtrace seems Qt-client specific, i.e., it's separate issue from gtk-client one.

#3 - 2020-04-16 10:28 AM - Marko Lindqvist
- File 0007-Qt-Fix-assert-failure-on-research-dialog-building-to.patch added
- Category set to gui-qt
- Status changed from New to Resolved
- Sprint/Milestone set to 3.1.0

Handling Qt-issue in this ticket. There's not enough information about gtk issue to distinguish it from other failures of the same assertion, so not opening new ticket for it until it's seen again - it might be already fixed.

Attached patch should fix the Qt issue.

#4 - 2020-04-16 11:59 PM - Marko Lindqvist
- Has duplicate Bug #860058: SEGV on unknown address (master, qt) added

#5 - 2020-04-18 09:51 AM - Marko Lindqvist
- Status changed from Resolved to Closed
- Assignee set to Marko Lindqvist

Files
0007-Qt-Fix-assert-failure-on-research-dialog-building-to.patch 1.86 KB 2020-04-16 Marko Lindqvist