# Freeciv - Bug #858212

## Qt heap-use-after-free entering Pick Nation screen (2.6.1+)

2020-02-02 07:33 AM - Chippo Elder

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th>Due date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Marko Lindqvist</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td>gui-qt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sprint/Milestone:</td>
<td>2.6.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

This BT/dump/thingy has appeared in another ticket #858069, but that ticket has 3 different dumps for between 3 and 5 different bugs and a completely inappropriate title.

To trigger it you need to compile with -fsanatize=address and I used llvm, but it should be the same with gcc. Then, sadly, you have to play for a while. Load a savegame, do a turn or two, start a New Game with a new ruleset, play a turn. Then when it's primed, Leave Game, Start New Game, don't touch anything (ruleset says default) except you click Pick Nation, and it dumps (which is quite pretty, with colours and all).

I can reliably reproduce it, but any exact written instructions never seem to work more than once.

chippo@chippo-Aspire-V3-731:~$ ASAN_OPTIONS="detect_leaks=0" freeciv-qt-26 -F
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "amplio2".
QSocketNotifier: Invalid socket 41 and type 'Read', disabling...
2: last message repeated 2 times
2: Loading tileset "delta2".

```
2826ERROR: AddressSanitizer: heap-use-after-free on address 0x6030027b16b8 thread T0
#0 0x99c5e3 in skip_intl_qualifier_prefix /home/chippo/Downloads/git_clones/freeciv/utility/fcintl.c:48:7
#1 0x845c3c in nation_set_by_rule_name /home/chippo/Downloads/git_clones/freeciv/common/nation.c:766:23
#2 0x726c40 in races_dialog::nationset_changed(int) /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/dialogs.cpp:984:10
#3 0x5924f0 in races_dialog::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/meta_dialogs.cpp:369:21
#4 0x7efc52df2e46 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x2b1467)
#5 0x7efc5270fc74 in QComboBox::currentIndexChanged(int) (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x270c74)
#6 0x7efc52712075 (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x273075)
#7 0x7efc5271489c (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x27589c)
#8 0x7efc52714af2 in QComboBox::setCurrentIndex(int) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x275af2)
#9 0x723098 in races_dialog::update_nationset_combo() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/dialogs.cpp:487:18
#10 0x720f6c in races_dialog::races_dialog(player*, QWidget*) /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/dialogs.cpp:414:3
#11 0x727708e in popup_races_dialog /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/dialogs.cpp:1034:23
#12 0x5a4170 in fc_client::slot_pick_nation() /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/pages.cpp:2045:3
#13 0x5564c8 in QtPrivate::FunctionPointer<void (fc_client::*)(), QtPrivate::List<>, void, void>(fc_client::*) /usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x25f2c7)
#14 0x5564c8 in void QtPrivate::FunctionPointer<void (fc_client::*)(), QtPrivate::List<>, void, void>(fc_client::*) /usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x25f2c7)
#15 0x55563c7 in QPrivateSignal::connectNotify(QObject*, QtPrivate::List<>, void)(fc_client::*) /usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x25f2c7)
#16 0x55563c7 in QPrivateSignal::connectNotify(QObject*, QtPrivate::List<>, void)(fc_client::*) /usr/lib/x86_64-linux-gnu/libQt5Core.so.5+0x25f2c7)
#17 0x7efc526fe235 in QAbstractButton::clicked(bool) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f235)
#18 0x7efc526fe45d (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f45d)
#19 0x7efc526f8a2 (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f8a2)
#20 0x7efc526fa64 in QAbstractButton::mouseReleaseEvent(QMouseEvent*) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f6a4)
#21 0x7efc526f404d in QWidget::event(QEvent*) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f404d)
#22 0x7efc526f8a8 in QApplicationPrivate::notify_helper(QObject*, QEvent*) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f8a8)
#23 0x7efc526f1305 in QApplication::notify(QObject*, QEvent*) (/lib64/x86_64-linux-gnu/libQt5Widgets.so.5+0x25f1305)
#24 0x7efc526fda99 in QCOREApplication::notifyInternal2(QObject*, QEvent*) (/lib64/x86_64-linux-gnu/libQt5Core.so.5+0x25f6a99)
```
prefix
Shadow bytes around the buggy address:
0x0c06804ee280: fd fd fd fd fa 00 00 00 00 fa 00 00 07 07
0x0c06804ee290: fa fd fd fd fa fd fd fd fa fd fa fd fd
0x0c06804ee2a0: fd fd fa 00 00 00 00 fa fd fd fa fd fd fa
0x0c06804ee2b0: 00 00 00 00 fa 00 00 00 00 fa fa fd fa
0x0c06804ee2c0: fa fd fd fa fd fd fa fd fd fa fd fd fa
0x0c06804ee2d0: fd fd fa fd fd fd fd fd fd fd fd fd
0x0c06804ee2e0: fd fd fa fd fd fa fd fd fd fa fd fd fa
0x0c06804ee2f0: fa fd fa fd fd fa fd fd fa fd fd fa fd fd
0x0c06804ee300: 00 00 00 00 fa fa fd fd fa fa fd fa fd
0x0c06804ee310: fd fd fd fa fa fd fa fd fd fa fa fd fa fd
0x0c06804ee320: fa fd fa fa fd fa 00 00 00 00 fa fa fd fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone:      f1
Stack mid redzone:       f2
Stack right redzone:     f3
Stack after return:      f5
Stack use after scope:   f8
Global redzone:          f9
Global init order:       f6
Poisoned by user:        f7
Container overflow:      fc
Array cookie:            ac
Intra object redzone:    bb
ASan internal:           fe
Left alloca redzone:     ca
Right alloca redzone:    cb
Shadow gap:              cc
2826ABORTING

Relatated issues:
Related to Freeciv - Bug #859139: Qt: Temporary QByteArrays often used after ...

History
#1 - 2020-02-02 09:20 PM - Marko Lindqvist
Which commit this was with? gui-qt/dialogs.cpp has changed several times recently (within a week) and I suspect those line numbers in your trace are not the same as in current S2_6 HEAD.

#2 - 2020-02-02 09:37 PM - Marko Lindqvist
Chippo Elder wrote:

Load a savegame, do a turn or two, start a New Game with a new ruleset, play a turn. Then when it's primed, Leave Game, Start New Game, don't touch anything (ruleset says default) except you click Pick Nation, and it dumps (which is quite pretty, with colours and all).

Do you use "Pick Nation" when starting the earlier games, or do you go by the random nation selection that is the default?

#3 - 2020-02-03 12:36 AM - Chippo Elder
Marko Lindqvist wrote:

Which commit this was with?

The dump I'm going to show you below is from 2.6.1+ (modified ec0f40dcfb), gui-qt client.

Marko Lindqvist wrote:

Do you use "Pick Nation" when starting the earlier games, or do you go by the random nation selection that is the default?

The latter. This is the first time during this program run that you touch the Pick Nation button.

So I followed my own instructions above and get this:

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".
QSocketNotifier: Invalid socket 41 and type 'Read', disabling...
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
=================================================================
==28888==ERROR: AddressSanitizer: heap-use-after-free on address 0x6030002b8598 thread T0
#0 0x9758f3 in skip_intl_qualifier_prefix /home/chippo/Downloads/git_clones/freeciv/utility/fcintl.c:48:7
#1 0x82f3cc in nation_set_by_rule_name /home/chippo/Downloads/git_clones/freeciv/common/nation.c:766:23
#2 0x719750 in races_dialog::nationset_changed(int) /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/dialogs.cpp:984:10
#3 0x592450 in races_dialog::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) /home/chippo/Downloads/git_clones/freeciv/client/gui-qt/meta_dialogs.cpp:369:21

2021-08-07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
@==28888==ABORTING
AddressSanitizer:DEADLYSIGNAL
Aborted (core dumped)

And since I worked out my ASAN core dump troubles, I can get a full backtrace:

Core was generated by `freeciv-qt-26'.
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 0x7f1a4e3baac0 (LWP 28888))]
(gdb) bt full
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
   set = {val = {0, 5106555, 895, 0, 0, 281470681751461, 0, 0, 0, 0, 0, 0, 0, 206158430216, 14073736201568}}
pid = <optimized out>
tid = <optimized out>
#1 0x0000771a5301c899 in __GI_abort () at abort.c:79
   save_stage = 1
act = 
   {__sigaction_handler = {sa_handler = 0x3fe6b5ce50b7821a, sa_sigaction = 0x3fe6b5ce50b7821a}, sa_mask = {__val = {0, 13975167971584, 13731440, 2, 2, 0, 0, 0, 0, 0, 0, 3, 0, 0}}, sa_flags = 0, sa_restorer = 0xc85e68 <__asan::error_message_buf_mutex>}
sigs = {__val = {32, 0 <repeats 15 times>}}
#2 0x000000000049e827 in ()
#3 0x000000000049f7801 in ()
#4 0x000000000049f3f89 in ()
#5 0x000000000049f3f89 in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, int, bool) ()
#6 0x000000000049e1d8 in __asan_report_load1 ()
#7 0x00000000009758f4 in skip_intl_qualifier_prefix (str=0x6030002b8598 "all") at fcintl.c:48
   ptr = <optimized out>
#8 0x000000000082f3cd in nation_set_by_rule_name (name=0x2 <error: Cannot access memory at address 0x2>) at nation.c:766
   qname = <optimized out>
#9 0x0000000000719751 in races_dialog::nationset_changed(int) (this=<optimized out>, index=<optimized out>) at dialogs.cpp:984
   rule_name = {static null = {<No data fields>}, d = 0x60300087bcb0}
poplon = 0x627000f7adb0
   rn = 0x6030002b8598 "all"
#10 0x00000000000952451 in races_dialog::qt_static_metacall(QObject*, QMetaObject::Call, int, void*)
   (o=0x2, _c=<optimized out>, _id=<optimized out>, _a=<optimized out>) at meta_dialogs.cpp:369
   _t = 0x2
#11 0x0000007f1a53d70468 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#12 0x0000007f1a53696c75 in QComboBox::currentIndexChanged(int) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#13 0x0000007f1a53699076 in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#14 0x0000007f1a5369b98d in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#15 0x0000007f1a5369b98d in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#16 0x0000007f1a536a1525 in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#17 0x0000007f1a537d0468 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#18 0x0000007f1a53696d66 in QComboBoxPrivateContainer::itemSelected(QModelIndex const&) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#19 0x0000007f1a536974fa in QComboBoxPrivateContainer::eventFilter(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#20 0x0000007f1a53d447ab in QCereApplicationPrivate::sendThroughObjectEventFilters(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#21 0x0000007f1a53550a75 in QCereApplicationPrivate::notify_helper(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#22 0x0000007f1a53550a53 in QCereApplication::notify(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#23 0x0000007f1a53d44a9a in QCereApplication::notifyInternal2(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Core.so.5
#24 0x0000007f1a53559157 in QCereApplicationPrivate::sendMouseEvent(QWidgetItem*, QMouseEvent*, QWidgetItem*, QWidget*, QWidget*, QWidget**, QQPointier<QWidgetItem>&, bool, bool) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#25 0x0000007f1a5355efad4 in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#26 0x0000007f1a535511d6 in () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#27 0x0000007f1a535590a86 in QCereApplicationPrivate::notify_helper(QObject*, QEvent*) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5

2021-08-07
I still don’t fully understand what happens here. If we're lucky, attached wild experiment helps, but I'm not surprised if it doesn't.

If the problem is in the lifetime of the temporary QByteArray when using construct like 'char *buf = str.toLocal8Bit().data()', the bad news is that Qt-client and ruledit code has lots of such usage. And I now think it's a bug in principle, even if this one is not about it.

grep -r "data()" client/qui-qt tools/ruledit

I still don’t fully understand what happens here. If we're lucky, attached wild experiment helps, but I'm not surprised if it doesn't.

I can't trigger it anymore. I tried a lot. The combination of the two patches (0007-Do-not-unqueue-mapview-updates-when-tileset-is-not-f.patch and QByteArrayLifetime.patch) has done the trick. Close the ticket.

In my efforts to discover why I no longer have a fixed-ghost-seen tree (and for simpler repeatability reasons), I dropped the QByteArrayLifetime.patch from my workflow. Now I'm being hit by use-after-free regularly. So I'm putting it back in.

This last one happened under quite different circumstances than earlier reported. I had been playing around in several savegames during that session in different rulesets etc. I had just started a New Game, had configured ruleset, players and difficulty. I had not gone into game options yet, 'cos that's where the Save is, and I want that ruleset to remember that I always want the Extended set of Nations. I was already in the choose-your-nation screen, fiddling with moving that window around on my screen and clicking all around on it, looking for I-dunno-what. Then I wanted to switch to Extended and clicked on the dropdown. It appeared in the correct place. I paused a good while, to take a screenshot, file it, and some other stuff. Then I clicked on Extended and the dump happened.

This BT looks very similar to the last, but there are some largish differences like the "set = {__val = {" values, so I'll include it here in case.
Core was generated by `freeciv-qt-26 -P'.
Program terminated with signal SIGABRT, Aborted.
#0  __GI_raise (sig=sig@entry=6) 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 0x7fd803b0eb80 (LWP 1282733))]
(gdb) bt full
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
set = 
  __val = {0, 281470681751461, 140724658498656, 140724658498656, 140724658498656, 5200464, 206158430216, 140724658499296, 140724658499104, 5111467, 140724658498720, 13250856, 140724658502544, 140724658502536, 140724658502448, 13849992}
pid = <optimized out>
tid = <optimized out>
#1  0x000007f8d808e6899 in __GI_abort () at abort.c:79
  save_stage = 1
  act =
    __sigaction_handler = {sa_handler = 0x400, sa_sigaction = 0x400},
    sa_mask = __val = {13850928, 140565873823744, 13850928, 2, 2, 2, 140724658499064, 140565873823840, 4686603, 2, 0, 0, 0, 0, 0, 0},
    sa_flags = 0,
    sa_restorer = 0xca3128 <__asan::error_message_buf_mutex>
  sigs = __val = {32, 0 <repeats 15 times>}
#2  0x00000000004fa157 in ()
#3  0x00000000004f8b31 in ()
#4  0x00000000004e06b9 in ()
#5  0x00000000004e1e2f in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, unsigned int, bool) ()
#6  0x00000000004e2508 in __asan_report_load1 ()
#7  0x00000000009510a4 in skip_intl_qualifier_prefix (str=0x603000723058 "all") at fcintl.c:48
  ptr = <optimized out>
#8  0x00000000007fa6ed in nation_set_by_rule_name (name=0x2 <error: Cannot access memory at address 0x2>) at nation.c:766
  qname = <optimized out>
#9  0x00000000007f28531 in races_dialog::nationset_changed(int) (this=optimized out), index=optimized out) at dialogs.cpp:984
  rule_name = [static null = {<No data fields>}, d = 0x6030000fd6b0]
  poption = 0x62700003fdb0
  rn = 0x603000723058 "all"
#10 0x0000000000593a11 in races_dialog::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) () at meta_dialogs.cpp:369
  t = 0x2
#11 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#12 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#13 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#14 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#15 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#16 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#17 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#18 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#19 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#20 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#21 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#22 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#23 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#24 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#25 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#26 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#27 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#28 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
#29 0x00000000007f6868 in QMetaObject::activate(QObject*, int, int, void**) () at /usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5
2021-08-07 7/10
I betcha that with the QByteArrayLifetime.patch applied, I don’t see this again.

#8 - 2020-02-06 01:55 PM - Chippo Elder

Seen in master, 3.0.32-dev (modified 5fa96c064c).

chippo@chippo-Aspire-V3-731:/home/chippo/Downloads/git_clones/freeciv/freeciv-dev/clinical.
c48:7
c766:23
]2 [63590 in races_dialog:nationset_changed(int) /home/chippo/Downloads/git_clones/freeciv/freeciv-dev/client/
[41079:10
]3 [700f50 in races_dialog:qt_static_metacall(QObject*, QMetaObject::Call, int, void**) /home/chippo/Dow
[4369:21
]4 [7d658d8467 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5C
]5 [7d651ec747 in QComboBox::setCurrentIndexChanged(int) (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x2
[70c74]
]6 [7d62010755 (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x273075)
]7 [7d620389bc (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x27589c)
]8 [7d62039bcb (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x2759bc)
]9 [7d6209524 (/usr/lib/x86_64-linux-gnu/libQt5Widgets.so.5+0x27b52c)
]10 [7d658d8467 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5C
]11 [7d651ec747 in QComboBoxPrivateContainer::itemSelected(QModelIndex const&) (/usr/lib/x86_64-linux-g
[12 [7d651ec747 in QComboBoxPrivateContainer::eventFilter(QObject*, QEvent*) (/usr/lib/x86_64-linux-gn
[13 [7d658d8467 in QMetaObject::activate(QObject*, int, int, void**) (/usr/lib/x86_64-linux-gnu/libQt5C
[14 [7d651ec747 in QApplicationPrivate::notify_helper(QObject*, QEvent*) (/usr/lib/x86_64-linux-gnu/lib
SUMMARY: AddressSanitizer: heap-use-after-free /home/chippo/Downloads/git_clones/freeciv/freeciv-dev/utility/fcintl.c:4817 in skip_intl_qualifier_prefix
Shadow bytes around the buggy address:
 0x0c068004fcb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fafa
I'm going to try the QByteArrayLifetime.patch and see if that helps.

#9 - 2020-02-06 04:20 PM - Chippo Elder
It applies cleanly in master and seems to do the job. I haven't managed to trigger this bug in master since applying it. I recommend that it gets committed.

#10 - 2020-02-07 07:07 PM - Marko Lindqvist
- Status changed from New to In Progress
- Assignee set to Marko Lindqvist
- Sprint/Milestone set to 2.6.2

Marko Lindqvist wrote:

... the lifetime of the temporary QByteArray when using construct like 'char *buf = str.toLocal8Bit().data()', the bad news is that Qt-client and ruledit code has lots of such usage.

-> Bug #859139

#11 - 2020-02-07 07:31 PM - Marko Lindqvist
- File 0008-Qt-Fix-heap-use-after-free-in-nations-dialog.patch added
- Status changed from In Progress to Resolved

Patch with commit message. No functional changes.

#12 - 2020-02-09 09:21 AM - Marko Lindqvist
- Status changed from Resolved to Closed

#13 - 2020-02-09 01:55 PM - Jacob Nevins
- Related to Bug #859139: Qt: Temporary QByteArrays often used after their lifetime has ended added

Files
<table>
<thead>
<tr>
<th>Patch Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>QByteArrayLifetime.patch</td>
<td>891 B</td>
<td>2020-02-03</td>
<td>Marko Lindqvist</td>
</tr>
<tr>
<td>0008-Qt-Fix-heap-use-after-free-in-nations-dialog.patch</td>
<td>1.28 KB</td>
<td>2020-02-07</td>
<td>Marko Lindqvist</td>
</tr>
</tbody>
</table>