Freeciv - Bug #858214
Ghost units seen, packhand assertion failure (2.6.1+, various clients)
2020-02-02 09:38 AM - Chippo Elder

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Marko Lindqvist</td>
</tr>
<tr>
<td>Category:</td>
<td>Server</td>
</tr>
<tr>
<td>Sprint/Milestone</td>
<td>2.6.2</td>
</tr>
<tr>
<td>Description</td>
<td>If you load the attached savegame in any client and press Turn Done, you'll see the following in the console:</td>
</tr>
</tbody>
</table>

chippo@chippo-Aspire-V3-731:~$ freeciv-qt-26 -F
2: Loading tileset "amplio2".
2: Loading tileset "deltax2".
2: Loading tileset "amplio2".
2: Loading tileset "amplio2".
1: 0x61200048cac0 1991 Settlers at (54,126) Tokugawa leysau
0: in handle_tile_info() [packhand.c::2947]: assertion '0 == unit_list_size(ptile->units)' failed.
0: Ghost units seen
0: Please report this message at https://www.hostedredmine.com/projects/freeciv
Aborted

chippo@chippo-Aspire-V3-731:~$ freeciv-gtk3.22-26 -F
2: Loading tileset "amplio2".
2: Loading tileset "deltax2".
2: Loading tileset "amplio2".
2: Loading tileset "amplio2".
1: 0x6120001996c0 1991 Settlers at (54,126) Tokugawa leysau
0: in handle_tile_info() [packhand.c::2947]: assertion '0 == unit_list_size(ptile->units)' failed.
0: Ghost units seen
0: Please report this message at https://www.hostedredmine.com/projects/freeciv
Aborted

Strangely, I'm not getting a core dump. I'm running with -F, ulimit -c is unlimited... must be some interaction with ASAN or something.
So no BT, but since it happens every time, you can try this at home.

Related issues:
- Has duplicate Freeciv - Bug #847413: Visibility of units loading without movi... Closed

History
#1 - 2020-02-02 12:50 PM - Chippo Elder
ASAN was, for unknown reasons, preventing a core dump. Without ASAN and with gcc, it behaves the same on that savegame, but now I get a core.

(gdb) bt full
#0 raise (sig=<optimized out>) at /sysdeps/unix/sysv/linux/raise.c:50
set = {__val = {0, 139665639218336, 0, 140730297286480, 140730297296821, 94354921019136, 7, 47244640256, 0,
1030513058584205668, 94354921020512, 0, 21474836480, 140730297286512, 140728898420736, 94354921020512})
pid = <optimized out>
tid = <optimized out>
#1 0x000055d0b6379617 in fc_assert_fail
(file=file@entry=0x55d0b63b5b24 "packhand.c", function=function@entry=0x55d0b63b7c00 "__FUNCTION__::31602" "handle_tile_info",
line=line@entry=2947, assertion=assertion@entry=0x55d0b63b6ba0 "0 == unit_list_size(ptile->units)", message=message@entry=0x55d0b63b5e55
"Ghost units seen") at log.c:523
level = LOG_FATAL
#2 0x000055d0b618ce10 in handle_tile_info (packet=packet@entry=0x55d0beb9ec0) at packhand.c:2985
new_known = TILE_KNOWN_UNSEEN
old_known = TILE_KNOWN_SEEN
known_changed = <optimized out>
tile_changed = <optimized out>
powner = <optimized out>
eowner = <optimized out>
presource = <optimized out>
pterrain = <optimized out>
ptile = <optimized out>

2021-08-07
FUNCTION = "handle_tile_info"
#3 0x000055d0b6120f73 in client_handle_packet (type=type@entry=PACKET_TILE_INFO, packet=packet@entry=0x55d0bebf9ec0) at packhand_gen.c:59
#4 0x000055d0b614a44f in client_packet_input (packet=packet@entry=0x55d0bebf9ec0, type=15) at client_main.c:770
FUNCTION = "client_packet_input"
#5 0x000055d0b6152593 in input_from_server (fd=fd@entry=41) at client_main.c:416
type = PACKET_TILE_INFO
packet = 0x55d0bebf9ec0
nb = <optimized out>
FUNCTION = "input_from_server"
#6 0x000055d0b614ac43 in client_main (argc=1, argv=0x7ffe53610f48) at client_main.c:685
i = 2
loglevel = LOG_NORMAL
ui_options = <optimized out>
ui_separator = <optimized out>
option = <optimized out>
fatal_assertions = 6
aii = 1
FUNCTION = "client_main"
#23 0x000055d0b6120f73 in __libc_start_main (main=0x55d0bebf9ec0, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7ffe53610f38) at csu/libc-start.c:308
result = <optimized out>
unwind_buf = (cancel_imp_buf = [[jmp_buf = {0, 370087417623776520, 94354895867824, 14073029729060, 0, 0, 7422477281803183880, 7417956425206094563}, mask_was_saved = 0}], priv = {pad = {0x0, 0x0, 0x7ffe53610f60, 0x7ffe672a72190}, data = {prev = 0x0, cleanup = 0x0, cancelctype = 1398869856}})
not_first_call = <optimized out>
#24 0x000055d0b614a44f in input_from_server at gui_main.cpp:114
#2 - 2020-02-02 09:41 PM - Marko Lindqvist
This kind of ghost unit issues are typically bugs in the server-side. It either sends units that it should not send, or does not send unit removal when it should.
#3 - 2020-02-02 09:57 PM - Marko Lindqvist
In the previous turn our Galleon sees the Japanese Settler id 1991 (that will turn to a ghost unit) and Trireme on the River tile on Japanese coast. At turn change our Galleon moves away.
Taking Japanese we can see that Settler 1991 has been loaded to the Trireme, and both of them have moved to the sea.
I don't know which happens first, and thus should hide the Settlers, moving of our Galleon away, or loading of the Settler to the Trireme.
#4 - 2020-02-02 10:08 PM - Marko Lindqvist
I suspect the problem being in that unit is not removed when it's loaded. Following is the backtrace taken when unit_transport_load_send() is called for unit 1991.
Breakpoint 1, unit_transport_load_send (punit=0x555555784ea70, ptrans=0x555555785170) at ../../src/server/unittools.c:2923
2923 unit_transport_load(punit, ptrans, FALSE);
(gdb) bt
#0 unit_transport_load_send (punit=0x555555784ea70, ptrans=0x555555785170) at ../../src/server/unittools.c:2923
#1 0x0000555555659a68 in handle_unit_load (pplayer=pplayer@entry=0x55555576021a0,
cargo_id=<optimized out>, trans_id=<optimized out>, tile_idx=<optimized out>)
at ../../../src/server/unithand.c:3380
#2 0x00005555555556863f6 in aiferry_gobyboat (ait=ait@entry=0x5555555975da0 <ai_types>,
pplayer=pplayer@entry=0x55555576021a0, punit=punit@entry=0x555555784ea70,
dest_tile=dest_tile@entry=0x55555584a45c0, with_bodyguard=with_bodyguard@entry=false)  
at ../../../src/server/unithand.c:830
#3 0x000055555555568f2bf in dai_gothere (ait=ait@entry=0x5555555975da0 <ai_types>,
pplayer=pplayer@entry=0x55555576021a0, punit=punit@entry=0x555555784ea70,
dest_tile=dest_tile@entry=0x55555584a45c0) at ../../../../src/ai/default/aitools.c:281
#4 0x000055555555568f140 in dai_auto_settler_run (ait=<optimized out>, pplayer=0x55555576021a0,  
punit=<optimized out>, state=0x555555576021a0, punit=<optimized out>) at ../../../../src/ai/default/aisettler.c:1043
#5 0x0000555555555c4d1 in auto_settlers_player (pplayer=pplayer@entry=0x555555576021a0)  
at ../../../../src/server/advisors/autosettlers.c:1162
#6 0x000055555555599358 in end_phase () at ../../../src/server/srv_main.c:1297
#7 0x000055555555599358 in end_phase () at ../../../src/server/srv_main.c:1297
#8 0x000055555555599358 in end_phase () at ../../../src/server/srv_main.c:1297
#9 0x000055555555599358 in end_phase () at ../../../src/server/srv_main.c:1297

#5 - 2020-02-02 10:17 PM - Marko Lindqvist
  - Status changed from New to In Progress
  - Assignee set to Marko Lindqvist
  - Sprint/Milestone set to 2.6.2

Unit can go out of sight when it moves. Usually that catches also unit loading, as it happens as the side effect of unit moving to the transport. But when unit loads to a transport on the same tile, there is no movement involved. Usually that happens within ones own city where other players don't see inside to begin with, but here the settler was loading to a trireme in the open (on a river tile).

#6 - 2020-02-02 10:45 PM - Marko Lindqvist
  - File 0005-Fix-ghost-unit-issue-when-unit-is-loaded-to-an-trans.patch added
  - Status changed from In Progress to Resolved

#7 - 2020-02-03 03:56 AM - Chippo Elder
You still get an unusual message on the console:
1: 0x61200048d9c0 1991 Settlers at (54,126) Tokugawa Ieyasu
But the message about ghosts is gone and so is the assert failure.

#8 - 2020-02-03 04:29 AM - Marko Lindqvist
Chippo Elder wrote:
  You still get an unusual message on the console:
  1: 0x61200048d9c0 1991 Settlers at (54,126) Tokugawa Ieyasu
You shouldn't, and I don't.

#9 - 2020-02-03 05:18 AM - Chippo Elder
Maybe that message is coming from a debug build which I'm also testing. Changing too many things at the same time...

#10 - 2020-02-03 06:16 AM - Chippo Elder
Now I must be going mad.
I do:

make clean
git pull

This give me 2.6.1+ (modified ec0f40dcbf). I have 3 locally applied patches:

diff --git a/client/gui-qt/dialogs.cpp b/client/gui-qt/dialogs.cpp
index 0901b432a0..b2017cac08 100644
--- a/client/gui-qt/dialogs.cpp
+++ b/client/gui-qt/dialogs.cpp
@@ -976,10 +976,15 @@ void notify_goto::inspect_city()
   void races_dialog::nationset_changed(int index)

2021-08-07
That's what I think I should have. So then I go through the sequence:

./autogen.sh
ASAN_OPTIONS="detect_leaks=0" CC="clang" CXX="clang++" CFLAGS="-fsanitize=address -fno-omit-frame-pointer -O1 -fno-optimize-sibling-calls -g -fPIE" CXXFLAGS="-fCFLAGS" ./configure --enable-client=all --enable-gitrev --dis
able-silent-rules --program-suffix=-26 --enable-debug=yes

make -j2

sudo make install

I run the gtk client with -F parameter, load the savegame in this ticket, press Turn Done and on the console I see:

chippo@chippo-Aspire-V3-731:~$ ASAN_OPTIONS="abort_on_error=1:disable_coredump=0:unmap_shadow_on_exit=1" freeciv-gtk3.22-26 -F

Encodings: Data=UTF-8, Local=UTF-8, Internal=UTF-8

2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "amplio2".
2: Loading tileset "amplio2".

1: 0x61200020d040 1991 Settlers at (54,126) Tokugawa Ieyasu

2: Backtrace:
2: 0: freeciv-gtk3.22-26(backtrace+0x5b) [0x4a3b6b]
2: 1: freeciv-gtk3.22-26(backtrace_print+0x112) [0x8ac052]
2: 2: freeciv-gtk3.22-26() [0x8a8e6bb]
2: 3: freeciv-gtk3.22-26(vdo_log+0x138) [0x8b8e578]
2: 4: freeciv-gtk3.22-26(do_log+0x19d) [0x8b8e653d]
2: 5: freeciv-gtk3.22-26(handle_tile_info+0xbd3) [0x5dc7f3]
2: 6: freeciv-gtk3.22-26(client_handle_packet+0x919) [0x5e8d7f3]
2: 7: freeciv-gtk3.22-26(client_packet_input+0x43) [0x564453]
2: 8: freeciv-gtk3.22-26(input_from_server+0x154) [0x5e6fe4]
2: 9: freeciv-gtk3.22-26() [0x519aa0]
2: 10: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x14e) [0x7fa62c97771e]
2: 11: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_contextDispatch+0xc6) [0x7fa62c977700]
2: 12: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_loop_run+0x83) [0x7fa62c977dc3]
2: 13: /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.gtk_main+0x7d) [0x7fa62d1c62c2d]
2: 14: freeciv-gtk3.22-26(ui_main+0x6b4) [0x515254]
2: 15: freeciv-gtk3.22-26(client_main+0x194a) [0x5636c8a]
2: 16: freeciv-gtk3.22-26(main+0x9) [0x514b99]
2: 17: /lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf3) [0x7fa62c70c1e3]
2: 18: freeciv-gtk3.22-26(_start+0x2e) [0x46c83e]

0: in handle_tile_info() [packhand.c::2947]: assertion '0 == unit_list_size(ptile->units)' failed.

2: Backtrace:
2: 0: freeciv-gtk3.22-26(backtrace+0x5b) [0x4a3b6b]
2: 1: freeciv-gtk3.22-26(backtrace_print+0x112) [0x8ac052]
2: 2: freeciv-gtk3.22-26() [0x8abebb]
2: 3: freeciv-gtk3.22-26(vdo_log+0x138) [0x8b6e578]
2: 4: freeciv-gtk3.22-26(do_log+0x19d) [0x8b6e653d]
2: 5: freeciv-gtk3.22-26(handle_tile_info+0xbd3) [0x5dc7f3]
2: 6: freeciv-gtk3.22-26(client_handle_packet+0x919) [0x5e8d7f3]
2: 7: freeciv-gtk3.22-26(client_packet_input+0x43) [0x564453]
2: 8: freeciv-gtk3.22-26(input_from_server+0x154) [0x5e6fe4]
2: 9: freeciv-gtk3.22-26() [0x519aa0]
2: 10: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x14e) [0x7fa62c97771e]
2: 11: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_contextDispatch+0xc6) [0x7fa62c977700]
2: 12: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_loop_run+0x83) [0x7fa62c977dc3]
2: 13: /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.gtk_main+0x7d) [0x7fa62d1c62c2d]
2: 14: freeciv-gtk3.22-26(ui_main+0x6b4) [0x515254]
2: 15: freeciv-gtk3.22-26(client_main+0x194a) [0x5636c8a]
2: 16: freeciv-gtk3.22-26(main+0x9) [0x514b99]

Ghost units seen

2: Backtrace:
2: 0: freeciv-gtk3.22-26(backtrace+0x5b) [0x4a3b6b]
2: 1: freeciv-gtk3.22-26(backtrace_print+0x112) [0x8ac052]
2: 2: freeciv-gtk3.22-26() [0x8abebb]
2: 3: freeciv-gtk3.22-26(vdo_log+0x138) [0x8b6e578]
2: 4: freeciv-gtk3.22-26(do_log+0x19d) [0x8b6e653d]
2: 5: freeciv-gtk3.22-26(fc_assert_fail+0xc6) [0x5e867f3]
2: 6: freeciv-gtk3.22-26(handle_tile_info+0xc2f) [0x5e8d7f3]
2: 7: freeciv-gtk3.22-26(client_handle_packet+0x919) [0x5e8d8c9]
2: 8: freeciv-gtk3.22-26(client_packet_input+0x43) [0x564453]
2: 9: freeciv-gtk3.22-26(input_from_server+0x154) [0x5e6fe4]
2: 10: freeciv-gtk3.22-26() [0x519aa0]
2: 11: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_context_dispatch+0x14e) [0x7fa62c97771e]
2: 12: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_contextDispatch+0xc6) [0x7fa62c977700]
2: 13: /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0(g_main_loop_run+0x83) [0x7fa62c977dc3]
2: 14: /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.gtk_main+0x7d) [0x7fa62d1c62c2d]
2: 15: freeciv-gtk3.22-26(ui_main+0x6b4) [0x515254]
2: 16: freeciv-gtk3.22-26(client_main+0x194a) [0x5636c8a]
2: 17: /lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf3) [0x7fa62c70c1e3]
2: 18: freeciv-gtk3.22-26(_start+0x2e) [0x46c83e]

2021-08-07
I've no idea what I was doing when I reported everything fixed. Or whether I'm doing something wrong now. Or what? But continuing, of course there's a core, so:

```
Core was generated by `freeciv-gtk3.22-26`.
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 0x7fa6295f5240 (LWP 671069))]
(gdb) bt full
#0  raise (sig=<optimized out>) at ../sysdeps/unix/sysv/linux/raise.c:50
set =
 ___val = {0, 0, 0, 0, 4607182418800017408, 0, 4607182418800017408, 0, 0, 0, 105690555242288, 0, 21
 474836480, 140733535349584, 140733193388032, 105759274701376})
#1 0x8b6836 in fc_assert_fail (file=<optimized out>, function=<optimized out>, line=<optimized out>
, assertion=<optimized out>, message=<optimized out>) at log.c:523
level = LOG_FATAL
#2 0x5e8dc9 in client_handle_packet (type=PACKET_TILE_INFO, packet=<optimized out>) at packhand_gen
.c:59
#3 0x564453 in input_from_server (fd=<optimized out>) at client.c:416
#4 0x56feit in get_net_input (source=<optimized out>, condition=<optimized out>, data=<optimized out>)
 at gui_main.c:2105
#5 0x7fa62c70c1e3 in _start+0x2e
```

Aborted (core dumped)

2021-08-07 6/8
The fix is in server side. Likely your client is not picking up correct (rebuilt) server to run, but runs some older build. And indeed you are using configure option --program-suffix, which I think won't work (-> I'll open a new ticket about that). Client does not launch the server by the name your new build has.

If your goal is to have multiple builds in parallel, use --prefix configure option. By using it, parallel versions of data files also gets installed. Also, when you set --prefix inside your home directory (or any other place where you have write permissions) you don't need to use 'sudo' when installing, removing the risk that your system gets completely broken by buggy freeciv install process.

Also, freeciv mostly works (localization does not work) out of build directory with no need to make install, if you launch it using ./fcgui and ./fcser wrapper scripts.

That is all really helpful advice. Thank you.

And you are correct. I have been trying to have multiple versions simultaneously installed, with more and less success. Confusion did happen and it has caused me to mal-report in tickets.

And knowing, now, how to run out of the build directory (.fcgui) means I can have as many consistent installed versions as I've got diskspace for. Yay!

But back to the issue of this ticket.

I start with a new directory.

```
$ git clone https://github.com/freeciv/freeciv.git
$ cd freeciv
$ git pull --all
$ git checkout S2_6
```

At this point, I would like to apply all three of those patches, but they don't apply, probably because one of them has already made it onto git. So, just apply the one about ghosts:

```
$ git apply ../../../0005-Fix-ghost-unit-issue-when-unit-is-loaded-to-an-trans.patch
```

Check where we are at.

```
$ git diff
diff --git a/server/unittools.c b/server/unittools.c
index 481231308a..9eb377825b 100644
--- a/server/unittools.c
+++ b/server/unittools.c
@@ -2913,11 +2913,27 @@
 static bool unit_enter_hut(struct unit *punit)
 { +
     bv_player can_see_unit;
+    fc_assert_ret(punit != NULL);
+    fc_assert_ret(ptrans != NULL);
+    BV_CLR_ALL(can_see_unit);
+    players_iterate(pplayer) {
+      if (can_player_see_unit(pplayer, punit)) {
+        BV_SET(can_see_unit, player_index(pplayer));
+      }
+    }
+    players_iterate_end;
+    unit_transport_load(punit, ptrans, FALSE);
+
+    BV_CLR_ALL(can_see_unit);
+    players_iterate(pplayer) {
+      if (BV_ISSET(can_see_unit, player_index(pplayer)) && !can_player_see_unit(pplayer, punit)) {
+        unit_goes_out_of_sight(pplayer, punit);
+      }
+    }
+    players_iterate_end;
+    send_unit_info(NULL, punit);
+    send_unit_info(NULL, ptrans);
```
So then

make clean
./autogen.sh
./configure --enable-client=qt,gtk3.22 --enable-gitrev --disable-silent-rules --enable-debug=some
make -j2
./fcgui

It brings up the gtk3.22 gui. How do I ask fcgui to launch to qt client?

I go and load the ghost savegame, and it bombs out with the assert and ghosts are yet again seen.

```
chippo@chippo-Aspire-V3-731:~/Downloads/freeciv-26$ ./fcgui
Unable to find client executable: freeciv
Searching for freeciv clients ...
... using ./client/freeciv-gtk3.22
Running ./client/freeciv-gtk3.22
2: Loading tileset "amplio2".
2: Loading tileset "delta2".
2: Loading tileset "amplio2".
2: Loading tileset "amplio2".
1: 0x55795d15bbc0 1991 Settlers at (54,126) Tokugawa Ieyasu
1: in handle_tile_info() [packhand.c::2947]: assertion '0 == unit_list_size(ptile->units)' failed.
1: Ghost units seen
1: Please report this message at https://www.hostedredmine.com/projects/freeciv
```

What's wrong with my recipe?

#13 - 2020-02-05 04:36 AM - Marko Lindqvist
Sorry, I forgot to mention one additional complication.

For security reasons, current directory is not part of the path client uses when searching for the server binary to launch in regular build. This limitation is lifted in --enable-debug builds.
Either build with --enable-debug, or install (with custom --prefix, as discussed earlier)

You can also test by running server manually, and using "Connect to Network Game" with host: "localhost" in the client.

#14 - 2020-02-05 06:18 AM - Chippo Elder
OK, confirmed.

The patch 0005-Fix-ghost-unit-issue-when-unit-is-loaded-to-an-trans.patch fixes this Ghost units issue. Commit the patch.

Marko Lindqvist wrote:

This limitation is lifted in --enable-debug builds.
Either build with --enable-debug, or install (with custom --prefix, as discussed earlier)

You mean with --enable-debug=yes or --enable-debug=checks. All my builds had at least --enable-debug=some (to avoid the evil -fomit-frame-pointer pulled in by --enable-debug=no) and this obviously does not lift the security limitation.

#15 - 2020-02-05 07:45 PM - Marko Lindqvist
- Status changed from Resolved to Closed

#16 - 2020-02-09 03:18 PM - Jacob Nevins
- Related to Bug #847413: Visibility of units loading without moving is not updated added

#17 - 2020-02-10 10:16 PM - Jacob Nevins
- Related to deleted (Bug #847413: Visibility of units loading without moving is not updated)

#18 - 2020-02-10 10:17 PM - Jacob Nevins
- Has duplicate Bug #847413: Visibility of units loading without moving is not updated added

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>ghost-coredump.sav.bz2</td>
<td>174 KB</td>
<td>2020-02-02</td>
<td>Chippo Elder</td>
</tr>
<tr>
<td>0005-Fix-ghost-unit-issue-when-unit-is-loaded-to-an-trans.patch</td>
<td>1.4 KB</td>
<td>2020-02-02</td>
<td>Marko Lindqvist</td>
</tr>
</tbody>
</table>

2021-08-07