

Freeciv - Bug #721949

AI passenger crash

2017-12-28 09:30 PM - Alexandro Ignatiev

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Marko Lindqvist	% Done:	0%
Category:	AI	Estimated time:	0.00 hour
Sprint/Milestone:	2.5.10		
Description			
<p>The client fails permanently. Playing in "Alien world" became nearly impossible since some turn as each turn or two it seems like server hangs up; client is active but after like a minute fails. In 2.5.3 version, it could hang for a minute or two if there were complicated task but then always worked.</p> <p>Then I tried to play default ruleset, but once it was also a failure (without so much hanging).</p> <p>Here go the console outputs (sorry, in Russian locale, but should be understandable). The second line from the bottom happened long before the program failed. The window-related issues are probably due to my attempts to scroll the "Traveller's report" which couldn't fit in the maximal accessible width of the sidebar. In gtk2 clients (2.5.3 and 2.6.0beta) I could always scroll the notepads from bookmark to bookmark if not all bookmarks fitted, here I couldn't (usually there are arrows and the sidebar can extend more, but scrolling by wheel still doesn't work).</p>			
<pre>#playing alien 2: Загрузка набора графики "amplio2". 2: Загрузка набора графики "hexemplio". 2: Загрузка набора графики "amplio2". 2: Загрузка набора графики "hexemplio". 2: предыдущее сообщение повторено 2 раза 2: Загрузка набора графики "alio". 1: Lost connection to server: ошибка чтения данных. #playing default 2: Загрузка набора графики "amplio2". 2: Загрузка набора графики "alio". 2: предыдущее сообщение повторено 2 раза 1: Lost connection to server: ошибка чтения данных. 2: Загрузка набора графики "amplio2". 2: Загрузка набора графики "alio". 2: Загрузка набора графики "hexemplio". 2: Загрузка набора графики "amplio2". 2: Загрузка набора графики "hexemplio". (freeciv-gtk3:5211): Gdk-CRITICAL **: gdk_window_move_resize_internal: assertion 'GDK_IS_WINDOW (window)' failed (freeciv-gtk3:5211): Gdk-CRITICAL **: gdk_window_move_resize_internal: assertion 'GDK_IS_WINDOW (window)' failed (freeciv-gtk3:5211): Gdk-CRITICAL **: gdk_window_move_resize_internal: assertion 'GDK_IS_WINDOW (window)' failed 1: Server wants us to remove unit id 753, but we don't know about this unit! 1: Lost connection to server: сервер прервал соединение.</pre>			
Related issues:			
Related to Freeciv - Bug #722271: Gdk-CRITICAL **: gdk_window_move_resize_int..		New	

History

#1 - 2018-01-01 03:47 PM - Jacob Nevins

- Related to Bug #722271: Gdk-CRITICAL **: gdk_window_move_resize_internal: assertion 'GDK_IS_WINDOW (window)' failed added

#2 - 2018-01-01 03:56 PM - Jacob Nevins

1: Server wants us to remove unit id 753, but we don't know about this unit!

This is not a good sign.

What version is this? 2.6.0-beta1?

#3 - 2018-01-01 04:04 PM - Jacob Nevins

fciv-T0168-Y01180-auto.sav.gz

Reproduced a server crash (segfault) with this one, with head of S2_6 (commit:152e9b037c), by just taking the human player and "Turn Done".

No sign of the message above in this case. Last bits of logs:

server:

```
...
3: [T169 - 2018/01/01 15:51:39] in send_packet_data() [/home/jtn/src/freeciv/git26/common/packets.c::213]: sending packet type=PACKET_TILE_INFO(15) len=10 to jtn
3: [T169 - 2018/01/01 15:51:39] in send_packet_data() [/home/jtn/src/freeciv/git26/common/packets.c::213]: last message repeated 2 times
3: [T169 - 2018/01/01 15:51:39] in send_packet_data() [/home/jtn/src/freeciv/git26/common/packets.c::213]: sending packet type=PACKET_UNIT_INFO(63) len=11 to jtn
3: [T169 - 2018/01/01 15:51:39] in unit_versus_unit() [/home/jtn/src/freeciv/git26/server/unittools.c::270]: sending packet type=PACKET_UNIT_INFO(63) len=11 to jtn
3: [T169 - 2018/01/01 15:51:39] in unit_versus_unit() [/home/jtn/src/freeciv/git26/server/unittools.c::270]: attack:45, defense:30, attack firepower:1, defense firepower:1
3: [T169 - 2018/01/01 15:51:39] in send_packet_data() [/home/jtn/src/freeciv/git26/common/packets.c::213]: sending packet type=PACKET_PLAYER_INFO(51) len=330 to jtn
```

Client:

```
...
3: in get_packet_from_connection() [/home/jtn/src/freeciv/git26/common/packets.c::517]: got packet type=(PACKET_TILE_INFO)15 len=10 from server
3: in get_packet_from_connection() [/home/jtn/src/freeciv/git26/common/packets.c::517]: last message repeated 2 times
3: in get_packet_from_connection() [/home/jtn/src/freeciv/git26/common/packets.c::517]: got packet type=(PACKET_UNIT_INFO)63 len=11 from server
3: in get_packet_from_connection() [/home/jtn/src/freeciv/git26/common/packets.c::517]: got packet type=(PACKET_UNIT_INFO)63 len=11 from server
3: in get_packet_from_connection() [/home/jtn/src/freeciv/git26/common/packets.c::517]: got packet type=(PACKET_PLAYER_INFO)51 len=330 from server
3: in sdl_audio_play() [/home/jtn/src/freeciv/git26/client/audio_sdl.c::108]: Playing file "data/stdmusic/CullamBruce-Lockhart--Dawning_Fanfare.ogg" on music channel
1: in client_conn_close_callback() [/home/jtn/src/freeciv/git26/client/clinet.c::136]: Lost connection to server: server disconnected.
```

Backtrace of server segfault:

```
#0 aiferry_gobyboat (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60, dest_tile=dest_tile@entry=0x1918c38, with_bodyguard=with_bodyguard@entry=false) at /home/jtn/src/freeciv/git26/ai/default/aiferry.c:873
    bodyguard = <optimised out>
    ferryboat = <optimised out>
    __FUNCTION__ = "aiferry_gobyboat"
#1 0x0000000000551457 in dai_gothere (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60, dest_tile=0x1918c38) at /home/jtn/src/freeciv/git26/ai/default/aitools.c:281
    __FUNCTION__ = "dai_gothere"
#2 0x0000000000554ce9 in dai_military_defend (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:959
    pcity = <optimised out>
    __FUNCTION__ = "dai_military_defend"
#3 0x000000000055b74 in dai_military_attack (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:1834
    dest_tile = 0x190e478
    id = 940
    ct = <optimised out>
    pcity = <optimised out>
```

```

__FUNCTION__ = "dai_military_attack"
#4 0x000000000559192 in dai_manage_military (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:2435
    id = 940
__FUNCTION__ = "dai_manage_military"
#5 0x00000000055aa70 in dai_manage_unit (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c55f60) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:2598
    bodyguard = <optimised out>
    is_ferry = <optimised out>
__FUNCTION__ = "dai_manage_unit"
#6 0x0000000005545398 in dai_manage_ferryboat (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c56250) at /home/jtn/src/freeciv/git26/ai/default/aiferry.c:1148
    boss = 0x1c55f60
    pcity = <optimised out>
    sanity = 939
    bossid = 940
    ptype = <optimised out>
__FUNCTION__ = "dai_manage_ferryboat"
#7 0x00000000055ba24 in dai_manage_unit (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0, punit=punit@entry=0x1c56250) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:2578
    bodyguard = <optimised out>
    is_ferry = true
__FUNCTION__ = "dai_manage_unit"
#8 0x00000000055ced0 in dai_manage_units (ait=ait@entry=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0) at /home/jtn/src/freeciv/git26/ai/default/aiunit.c:2746
    punit = 0x1c56250
    punit_numbers = 0x7ffea10d1ec8
    punit_index = <optimised out>
__FUNCTION__ = "dai_manage_units"
#9 0x0000000005547b8d in dai_do_first_activities (ait=0xa3aee0 <ai_types>, pplayer=pplayer@entry=0x36339f0) at /home/jtn/src/freeciv/git26/ai/default/aihand.c:745
No locals.
#10 0x000000000515300 in cai_do_first_activities (pplayer=0x36339f0) at /home/jtn/src/freeciv/git26/ai/classic/classicai.c:438
No locals.
#11 0x00000000043fafa in ai_start_phase () at /home/jtn/src/freeciv/git26/server/srv_main.c:935
    _plr_ = 0x36339f0
    MY_i = 47
    pplayer = 0x36339f0
#12 begin_phase (is_new_phase=<optimised out>) at /home/jtn/src/freeciv/git26/server/srv_main.c:1125
No locals.
#13 srv_running () at /home/jtn/src/freeciv/git26/server/srv_main.c:2660
    save_counter = <optimised out>
    i = <optimised out>
    is_new_turn = <optimised out>
    skip_mapimg = <optimised out>
    need_send_pending_events = false
#14 srv_main () at /home/jtn/src/freeciv/git26/server/srv_main.c:3283
__FUNCTION__ = "srv_main"
#15 0x00000000043521a in main (argc=20, argv=0x7ffea10d21f8) at /home/jtn/src/freeciv/git26/server/civserver.c:476
    inx = 20
    showhelp = <optimised out>
    showvers = <optimised out>
    option = <optimised out>
__FUNCTION__ = "main"

```

My aiferry.c:873 is:

```

/* We are in still transit */
def_ai_unit_data(punit, ait)->done = TRUE;

```

#4 - 2018-01-01 04:30 PM - Marko Lindqvist

There's no AI data structures for punit. It's because it's already dead (i.e, bug is that pointer to an already dead unit is still used):

```

(gdb) p unit_is_alive(punit)
$4 = false

```

#5 - 2018-01-01 04:34 PM - Jacob Nevins

freeciv-T0173-Y00289-auto.sav.gz

I've not been able to reproduce any obvious trouble with this one just by hitting "Turn Done", either with head-of-S2_6 or 2.6.0-beta1. I've not seen the "don't know about this unit" message at all (I acknowledge that you said it happened long before the crash).

```
(freeciv-gtk3:5211): Gdk-CRITICAL **: gdk_window_move_resize_internal: assertion 'GDK_IS_WINDOW (window)' failed
```

I think this is unrelated to your crashes. I've seen other reports. I've raised a separate ticket, bug [#722271](#), about it; if you have any more detail about how to reproduce it to put there, that would be useful.

#6 - 2018-01-01 05:00 PM - Marko Lindqvist

Marko Lindqvist wrote:

There's no AI data structures for punit. It's because it's already dead (i.e. bug is that pointer to an already dead unit is still used):

```
(gdb) p unit_is_alive(punit)
$4 = false
```

dai_amphibious_goto_constrained() comment says:

```
/* It is theoretically possible passenger died here due to      * autoattack against another passing unit at its location. */
```

When that happens, dai_amphibious_goto_constrained() still returns TRUE.

#7 - 2018-01-01 05:26 PM - Marko Lindqvist

- File 0001-Fix-crash-when-former-ferry-leader-activates.patch added
- File 0001-Fix-crash-when-former-ferry-leader-activates.patch added
- Subject changed from Constant gtk3 client connection losses to AI passenger crash
- Category set to AI
- Status changed from New to Resolved
- Sprint/Milestone changed from 2.6.0-beta2 to 2.5.10

#8 - 2018-01-04 02:11 PM - Marko Lindqvist

- Status changed from Resolved to Closed
- Assignee set to Marko Lindqvist

Files

fciv-T0168-Y01180-auto.sav.gz	80.5 KB	2017-12-28	Alexandro Ignatiev
freeciv-T0173-Y00289-auto.sav.gz	133 KB	2017-12-28	Alexandro Ignatiev
0001-Fix-crash-when-former-ferry-leader-activates.patch	1.36 KB	2018-01-01	Marko Lindqvist
0001-Fix-crash-when-former-ferry-leader-activates.patch	1.37 KB	2018-01-01	Marko Lindqvist