Freeciv - Bug #830553

Qt client may crash when setting a rally point and the city is lost

2019-08-06 10:14 PM - Louis Moureaux

<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>Jacob Nevins</td>
</tr>
<tr>
<td>Category:</td>
<td>gui-qt</td>
</tr>
<tr>
<td>Sprint/Milestone</td>
<td>2.6.2</td>
</tr>
</tbody>
</table>

**Description**

Steps to reproduce:

- In the Qt client, start setting a rally point, select an empty size 1 city near a border
- With another instance to wipe the city with the other player (or remove it in edit mode)
- In the first client, click anywhere on the map

The Qt client crashes because it tries to access the position of a city that has been freed (https://github.com/freeciv/freeciv/blob/master/client/gui-qt/mapctrl.cpp#L269).

Qt client's rally points were first seen in 2.6. A proper fix will also require changes to the common code. I'll come up with a minimal patch for this branch.

In 3.0 and later it should be fixed together with the transition to server-side rally points (#822927).

**Related issues:**

- Related to Freeciv - Feature #822927: Rally points for cities
  - Closed
- Related to Freeciv - Bug #858746: Setting a rally point out of the map crashe...
  - Closed

**History**

**#1 - 2019-08-06 10:15 PM - Louis Moureaux**

- Related to Feature #822927: Rally points for cities added

**#2 - 2019-08-06 11:11 PM - Louis Moureaux**

In 3.0 and later it should be fixed together with the transition to server-side rally points (#822927).

Just realized that server-side RP didn't make it to 3.0. Hopefully a patch similar to the one for 2.6 can be used.

**#3 - 2019-12-18 12:35 PM - Jacob Nevins**

- Sprint/Milestone changed from 2.6.1 to 2.6.2

**#4 - 2020-02-03 09:15 PM - Louis Moureaux**

- File 0001-Fix-crashes-in-Qt-client-side-rally-points.patch added

Patch for 2.6 and 3.0

**#5 - 2020-02-03 10:24 PM - Jacob Nevins**

(Patch contains strings, so we want it on S2_6 by end of Thursday to meet 2.6.2 string freeze.)

**#6 - 2020-02-04 08:47 AM - Chippo Elder**

So how do you go about testing this patch from one machine?

I started a server, set minplayers to 2 and aifill to 0. Started two qt clients. The first one connects to the server no problem. The second one won't, and the server's console says:

2: Connection request from chippo from chippo-Aspire-V3-731
2: c3 has client version 2.6.1+
2: Client rejected: c3 from chippo-Aspire-V3-731 (connection incomplete).
2: chippo was rejected: Duplicate login name [chippo-Aspire-V3-731].
2: Lost connection: c3 from chippo-Aspire-V3-731 (rejected).

What? It can't be using my ip address as my unique key! It must be ip-addr/src-port.

So, what do you do? How can I test this patch with only one machine?

#7 - 2020-02-04 08:50 AM - Chippo Elder
Oops. Already resolved. This idiot here, overuses 'chippo' for machines, logins, people, everything.

I just had to change the username and all's going fine.

#8 - 2020-02-04 10:03 AM - Chippo Elder
- File rally-city.sav.bz2 added
- File rally-city.png added

I can't replicate the original problem.

The attached savegame is for 2 human players, 'chip' and 'chop'. If you connect with chop, you'll see that the Settler [l tgt="unit" id=116 name="Settlers"/] has a rally point on the city [l tgt="city" id=118 name="Lakam Ja'"/] for it's Go-To to [l tgt="city" id=115 name="Yax Mutal"/].

Connected as chip, you'll see have a Centurion standing next to Lakam Ja'. Press Turn done a few times in each client, destroying the city with your Centurion. A turn or two later, check out the Settler's orders. They look fine. See attached screenshot.

This is all 2.6.1+ (modified 7c30e20232), gui-qt client (unpatched).

#9 - 2020-02-05 09:48 AM - Jacob Nevins
- Status changed from New to Resolved
- Assignee set to Jacob Nevins

I can't replicate the original problem. […]

I think the problem is before that point -- specifically when a city goes away while the user is still selecting a rally point for its future units.

Once a city has made a unit and given it goto orders, as in this case, the city's rally point is irrelevant to it.

I can replicate trouble from your savegame:

1. As chip: Multiplayer / Set/unset rally point
2. As chip: click on Lakam Ja'
3. As chop: destroy Lakam Ja'
4. As chip: click somewhere on the map

(It didn't crash for me, but it said "Tile (70, 17) set as rally point from city @��f���." so clearly it was unhappy. Louis' patch fixed the issue.)

#10 - 2020-02-05 09:50 AM - Jacob Nevins
...so I plan to commit the patch to S2_6/S3_0 soon.

(Louis said on IRC that the originally reported crash is already fixed on master; there is another crash fixed by this patch that causes an assertion failure on master, apparently. That probably wants another ticket.)

#11 - 2020-02-05 04:34 PM - Louis Moureaux
Jacob Nevins wrote:

...so I plan to commit the patch to S2_6/S3_0 soon.

(Louis said on IRC that the originally reported crash is already fixed on master; there is another crash fixed by this patch that causes an assertion failure on master, apparently. That probably wants another ticket.)

-> #858746

#12 - 2020-02-05 09:49 PM - Jacob Nevins

2022-08-20 2/3
- Related to Bug #858746: Setting a rally point out of the map crashes the Qt client added

#13 - 2020-02-05 10:02 PM - Jacob Nevins
- Status changed from Resolved to Closed

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-Fix-crashes-in-Qt-client-side-rally-points.patch</td>
<td>4.51 KB</td>
<td>2020-02-03</td>
<td>Louis Moureaux</td>
</tr>
<tr>
<td>rally-city.sav.bz2</td>
<td>14.5 KB</td>
<td>2020-02-04</td>
<td>Chippo Elder</td>
</tr>
<tr>
<td>rally-city.png</td>
<td>647 KB</td>
<td>2020-02-04</td>
<td>Chippo Elder</td>
</tr>
</tbody>
</table>