Freeceiv - Bug #919308
Initiating patrol order on units with limited fuel crashes the client under some circumstances

2021-02-06 11:21 PM - Alina L.

<table>
<thead>
<tr>
<th>Status: Closed</th>
<th>Start date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority: Normal</td>
<td>Due date:</td>
</tr>
<tr>
<td>Assignee: Marko Lindqvist</td>
<td>% Done: 0%</td>
</tr>
<tr>
<td>Category: Client</td>
<td>Estimated time: 0.00 hour</td>
</tr>
<tr>
<td>Sprint/Milestone: 2.6.4</td>
<td></td>
</tr>
</tbody>
</table>

Description

Happened in the gtk3.22 client built from S3_1, commit 9664b134. Tested on two air units in a custom ruleset, each with fuel for two turns, copied from the experimental/goldkeep ruleset's AWACS and Bomber, starting from a city.

Selecting "Patrol", either from the "Unit" menu, or by pressing "Q", while the mouse cursor is hovering over a tile close enough to reach within a turn, but not close enough to reach and return to a refuel point, crashes the client with a segfault.

Selecting the command while closer and then moving the cursor out does not crash the client (just displays an "invalid goto" cursor).

Selecting the command while further out does not immediately crash the client (displaying an "invalid goto" cursor), but bringing the cursor closer in then crashes the client.

In short:

- When starting within range move_rate/2, everything is fine
- When starting outside that range, crashes as soon as the cursor enters range move_rate

Note that this was observed and tested on units with fuel for two turns, so they could theoretically fly out one turn and return the next (when doing it by hand).

History

#1 - 2021-02-06 11:24 PM - Alina L.
Just did another test: The crash does not seem to happen with units that only have fuel for a single turn (in this case, a stealth fighter).

#2 - 2021-02-09 11:44 AM - Marko Lindqvist
Reproduced in S3_1 HEAD with experimental ruleset

Thread 1 "freeceiv-gtk3.22" received signal SIGSEGV, Segmentation fault.

pf_path_last_position (path=path@entry=0x0)
at ../../../../src/common/aicore/path_finding.c:3499

3499 return path->positions + (path->length - 1);
(gdb) bt
#0 pf_path_last_position (path=path@entry=0x0)
at ../../../../src/common/aicore/path_finding.c:3499
#1 0x0000555555555d1b73 in update_last_part
(goto_map=0x5555555802f0, ptile=ptile@entry=0x55555788b5e0)
at ../../../src/client/goto.c:349
#2 0x0000555555555d341c in is_valid_goto_draw_line (dest_tile=0x55555788b5e0)
at ../../../src/client/goto.c:1336
#3 0x0000555555555d2500 in update_line (canvas_x=<optimized out>, canvas_y=<optimized out>)
at ../../../src/client/mapctrl_common.c:669
#4 0x0000555555565758d in create_line_at_mouse_pos ()
at ../../../src/client/gui-gtk-3.22/mapctrl.c:363
...

#3 - 2021-02-09 11:57 AM - Marko Lindqvist
- Category changed from gui-gtk-3.22 to Client
- Status changed from New to In Progress
- Sprint/Milestone set to 2.6.4

#4 - 2021-02-09 03:47 PM - Marko Lindqvist
- File 0011-Fix-client-crash-on-setting-up-patrol-for-fuel-1-uni.patch added
- Status changed from In Progress to Resolved
#5 - 2021-02-13 08:12 PM - Marko Lindqvist

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

<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0011-Fix-client-crash-on-setting-up-patrol-for-fuel-1-uni.patch</td>
<td>1.18 KB</td>
<td>2021-02-09</td>
<td>Marko Lindqvist</td>
</tr>
</tbody>
</table>