Freeciv - Bug #874452

AI EFT_DEFEND_BONUS evaluation illegal read with ocean cities

2020-05-20 08:29 PM - Marko Lindqvist

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marko Lindqvist	**% Done:**	0%
Category:	AI	**Estimated time:**	0.00 hour
Sprint/Milestone:	2.6.3		

Description

Running autogame of rather old codebase on valgrind:

```
78750 Invalid read of size 1
78750    at 0x27AEF4: dai_effect_value (daieffects.c:486)
78750    by 0x254898: adjust_improvement_wants_by_effects (aicity.c:1642)
78750    by 0x254898: dai_build_adv_adjust (aicity.c:1909)
78750    by 0x177C79: building_advisor (advbuilding.c:264)
78750    by 0x250FA7: dai_manage_cities (aicity.c:877)
78750    by 0x25C19D: dai_do_last_activities (aihand.c:772)
78750    by 0x152D3C: end_phase (srv_main.c:1336)
78750    by 0x152D3C: srv_running (srv_main.c:2792)
78750    by 0x152D3C: srv_main (srv_main.c:3349)
78750    by 0x147884: main (civserver.c:482)
78750  Address 0xd2106ff is 1 bytes before a block of size 38 alloc'd
78750    at 0x483677F: malloc (vg_replace_malloc.c:309)
78750    by 0x37E763: fc_real_malloc (mem.c:89)
78750    by 0x37E8C8: fc_real_calloc (mem.c:137)
78750    by 0x178C55: adv_data_phase_init (advdata.c:280)
78750    by 0x15248A: begin_phase (srv_main.c:1199)
78750    by 0x15248A: srv_running (srv_main.c:2709)
78750    by 0x15248A: srv_main (srv_main.c:3349)
78750    by 0x147884: main (civserver.c:482)
78750
78750 Invalid read of size 1
78750    at 0x27B211: dai_effect_value (daieffects.c:493)
78750    by 0x254898: adjust_improvement_wants_by_effects (aicity.c:1642)
78750    by 0x254898: dai_build_adv_adjust (aicity.c:1909)
78750    by 0x177C79: building_advisor (advbuilding.c:264)
78750    by 0x250FA7: dai_manage_cities (aicity.c:877)
78750    by 0x25C19D: dai_do_last_activities (aihand.c:772)
78750    by 0x152D3C: end_phase (srv_main.c:1336)
78750    by 0x152D3C: srv_running (srv_main.c:2792)
78750    by 0x152D3C: srv_main (srv_main.c:3349)
78750    by 0x147884: main (civserver.c:482)
78750  Address 0xd2106ff is 1 bytes before a block of size 38 alloc'd
78750    at 0x483677F: malloc (vg_replace_malloc.c:309)
78750    by 0x37E763: fc_real_malloc (mem.c:89)
78750    by 0x37E8C8: fc_real_calloc (mem.c:137)
78750    by 0x178C55: adv_data_phase_init (advdata.c:280)
78750    by 0x15248A: begin_phase (srv_main.c:1199)
78750    by 0x15248A: srv_running (srv_main.c:2709)
78750    by 0x15248A: srv_main (srv_main.c:3349)
78750    by 0x147884: main (civserver.c:482)
```

daieffects.c:486 in this codebase is:
`if ((place && ai->threats.continent[place])`

daieffects.c:493 is:
`if (place && ai->threats.continent[place]) {`

I assume this to be a problem with an ocean city -> continent 'place' being negative.

History

#1 - 2020-05-20 10:09 PM - Marko Lindqvist

- File 0028-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch added

- File 0012-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch added

- File 0010-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch added

- Status changed from New to Resolved

- Sprint/Milestone set to 2.6.3

#2 - 2020-05-25 02:48 AM - Marko Lindqvist

- Status changed from Resolved to Closed

- Assignee set to Marko Lindqvist

Files

0028-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch	1.42 KB	2020-05-20	Marko Lindqvist
0012-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch	1.42 KB	2020-05-20	Marko Lindqvist
0010-AI-Fix-illegal-read-on-EFT_DEFEND_BONUS-evaluation-w.patch	1.41 KB	2020-05-20	Marko Lindqvist