**Freeciv - Bug #864613**

**action fail dice roll odds can be outside its range**

2020-03-13 08:47 AM - Sveinung Kvilhaugsvik

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Sveinung Kvilhaugsvik</td>
<td>% Done: 0%</td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td>General</td>
<td>Estimated time: 0.00 hour</td>
<td></td>
</tr>
<tr>
<td>Sprint/Milestone:</td>
<td>3.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Discovered while reading:
https://github.com/Lexxie952/fcw.org-server/commit/d64b010b69a367bc4699b1b38fc5c98b16db044d#diff-b6b1d12fd9a51d2bd5093289d36e2e96R1611

**History**

**#1 - 2020-03-13 09:01 AM - Sveinung Kvilhaugsvik**
- File 3.x.patch added
- Status changed from In Progress to Resolved
- Sprint/Milestone changed from 2.6.3 to 3.0.0

**#2 - 2020-04-05 11:54 PM - Lexxie L**

It is weird that you have read this commit without noticing or commenting about the really huge problem that was fixed. The backdoor Poison Exploit where you can never fail. Warning: not fixing this is EXCEPTIONALLY BAD.

**#3 - 2020-04-06 05:55 AM - Sveinung Kvilhaugsvik**

- Status changed from Resolved to Closed

It can fail if the city has a diplomatic defender. I have already added another action, "Spread Plague", that is almost the same as "Poison City" except that it can fail because of dipchance and that it activates Freeciv's plague system. Please file a new issue if you want dipchance-failure without plague activation.

**#4 - 2020-04-06 08:16 AM - Chippo Elder**

Your commit caused the following warning to appear during the build:

```c
actions.c:3344:1: warning: control may reach end of non-void function [-Wreturn-type]
} ^
1 warning generated.
```

But I can't understand why this warning wasn't always being generated, or why the commit encouraged it to be noticed by the compiler - it's thousands of lines away.

**#5 - 2020-04-06 08:42 AM - Marko Lindqvist**

Chippo Elder wrote:

Your commit caused the following warning to appear during the build: [...] But I can't understand why this warning wasn't always being generated, or why the commit encouraged it to be noticed by the compiler - it's thousands of lines away.

Which compiler and options?

My guess is that change of length of the modified function resulted in a change in inlining behavior, which in turns means compiler no longer gets the benefit of knowing the behavior of the called function when it tries to figure out if the flow can reach the end or not.

**#6 - 2020-04-06 10:13 AM - Chippo Elder**

Marko Lindqvist wrote:

Which compiler and options?

2021-08-05
"clang version 9.0.0-2 (tags/RELEASE_900/final)" and my configure had CFLAGS="-g -O3" and --enable-debug=no. No -Wanything or my usual -fsanitize... I wonder...

I normally compile with UBSan and ASan and checks and everything. Maybe this warning has nothing to do with the commit, and it only gets noticed by the compiler when you're doing -O3 and whatever --enable-debug=no pulls in.

#7 - 2020-04-06 10:21 AM - Chippo Elder
Chippo Elder wrote:

I normally compile with UBSan and ASan and checks and everything. Maybe this warning has nothing to do with the commit, and it only gets noticed by the compiler when you're doing -O3 and whatever --enable-debug=no pulls in.

Yup. The warning goes away when I do a 'normal' compile, which in my case is

ASAN_OPTIONS="detect_leaks=0" CC="clang" CXX="clang++" CFLAGS="-fsanitize=undefined -fsanitize=address -fno-omit-frame-pointer -O1 -fno-optimize-sibling-calls -g -fPIE" CXXFLAGS="$CFLAGS" ./configure --enable-client=all --enable-fcdb=all --enable-gitrev --program-suffix=-30 --enable-debug=some

#8 - 2020-04-17 12:02 PM - Lexxie L
Sveinung Kvilhaugsvik wrote:

It can fail if the city has is a diplomatic defender. I have already added another action, "Spread Plague", that is almost the same as "Poison City" except that it can fail because of diplchance and that it activates Freeciv's plague system. Please file a new issue if you want diplchance-failure without plague activation.

Can you show me where in the documentation to community players it is explained that poisoning city is exempt from diplchance and is a golden road to get endless free promotions or use army of spies to get no risk promotions and completely lay waste to any enemy city not protected by comparably sized army of enemy spies? It's scandalous. People on the community front lines of teaching new players and running servers with lots of active games face things like PR crisis because of these kinds of arbitrary "backroom decisions" outside the documentation or common sense.

#9 - 2020-04-17 12:20 PM - Marko Lindqvist
Lexxie L wrote:

documentation to community players

I'd like to see any document (even code comment) that it's, or has ever been, intentional feature and not a bug. Until then I'd treat it as a bug.

#10 - 2020-04-17 10:14 PM - Sveinung Kvilhaugsvik
Marko Lindqvist wrote:

Lexxie L wrote:

documentation to community players

I'd like to see any document (even code comment) that it's, or has ever been, intentional feature and not a bug. Until then I'd treat it as a bug.

I too believed this was an unintentional bug when I first saw it. Then I discovered that the header of its action performer function doesn't mention a failure dice roll. The functions of diplomatic actions when the player must beat diplchance mentions it. Than I discovered that this is what civ2, according to my understanding of http://home.tiscali.cz:8080/~cz045662/civ2/dipspy.htm, did.

Making this ruleset controlled (and auto documented) has been on my TODO-list for many years. (I too find this rule surprising.) I only got around to documenting diplomatic battle causing. I have filed Feature #869738 so making it ruleset controlled will be done in time for 3.1. I have filed Feature #869739 for the documentation part.

#11 - 2020-04-20 08:24 PM - Marko Lindqvist
Sveinung Kvilhaugsvik wrote:

I discovered that this is what civ2, according to my understanding of http://home.tiscali.cz:8080/~cz045662/civ2/dipspy.htm, did.

So it comes with civ2 compatibility. At least in civ2 ruleset it then should not be changed.

Making this ruleset controlled (and auto documented) has been on my TODO-list for many years. (I too find this rule surprising.) I only got around to documenting diplomatic battle causing. I have filed Feature #869738 so making it ruleset controlled will be done in time for 3.1. I have filed...
Feature #869739 for the documentation part.

These still leave static documentation, especially in stable branches that are not getting the autodocumentation part, confusing. I opened Feature #870009 for that part.

Is there other diplomat/spy actions that are not subject to diplchance when one would assume them to be? (Establishing embassy comes to mind as something that does not surprise me, but still something someone could assume affected after reading diplchance documentation)

#12 - 2020-04-20 09:34 PM - Marko Lindqvist

The lack of base roll probably turned to a problem in respect to diplchance with this 2005 commit:

commit fc33bd0b13ff8bf935babd448bb68236f7f53449
Author: Per I. Mathisen <per@leftist.net>
Date: Mon May 2 19:05:15 2005 +0000

Make diplomat combat not depend on diplchance. ... See PR#12896.

Before that diplchance was affecting even those actions that lack base roll via its effect on diplomatic battle part of the attempt.

#13 - 2020-04-21 12:14 AM - Lexxie L

Thanks for follow-up answers. It seems civ2 still had a few rough edges in it that don't survive the test of time.

Files

| 3.x.patch | 1.01 KB | 2020-03-13 | Sveinung Kvilhaugsvik |