New issue

Jump to bottom

Invalid generators were not removed from zone list #810

Merged derselbst merged 2 commits into 2.1.x from issue808 on Mar 15, 2021

Conversation 19 Commits 2 Checks 18 Files changed 1

derselbst commented on Mar 14, 2021 Member

`fluid_list_remove()` should receive the beginning of a list, so it can adjust the predecessor of the element to be removed. Otherwise, the element would remain in the list, which in this case led to a use-after-free afterwards.

Resolves #808

`Invalid generator were not removed from list` ··· ✕ 67596a8

derselbst added the bug label on Mar 14, 2021

derselbst added this to the 2.1 milestone on Mar 14, 2021

derselbst requested a review from mawe42 last year

derselbst commented on Mar 14, 2021 Member Author

@veritas501 You may give it a test.

veritas501 commented on Mar 14, 2021

Okay. It seems that the old bug has been fixed. I'm still testing if there are more bugs. @derselbst

👍 1

mawe42 commented on Mar 14, 2021 • edited Member

I must admit I don't understand why this fixes the bug. `*hz` is a pointer to the first element in the zone list. So at the start it's effectively identical to the new `start_of_zone_list`. And `*hz` only gets changed if we encounter a global zone that is not first in list. In this case, the global zone moved to be first in that list and `*hz` is updated accordingly. So doing a `fluid_list_remove` on `*hz` should have the same effect as on the new `start_of_zone_list` pointer, shouldn't it?

derselbst commented on Mar 14, 2021 Member Author

> *hz is a pointer to the first element in the zone list.

No, `hz` is a pointer to pointer. `*hz` is (usually) equal to `p2`. So, it would have been like putting

```
fluid_list_remove(p2, p2->data);
```

mawe42 commented on Mar 14, 2021 Member

Ah, of course! Hm... then I have a hard time understanding the purpose of `hz` in the first place, and when it gets updated. I guess I need more time going through this again. That code reads a little like it's been deliberately obfuscated :-) I once had the impression that I understand what's going on, but that was a long time ago...

derselbst commented on Mar 14, 2021 Member Author

The purpose of `hz` is not quite clear to me as well. It could be a leftover when they passed `hz` to a separate function that removed the zone:

fluidsynth/fluidsynth/src/sfloader/fluid_defsfont.c
Line 2443 in 62e375c

```
2443    sfont_zone_delete (sf, hz, (SFZone *) (p2->data));
```

The core logic around it already exists since "Initial Revision", so I'm a bit cautious to touch it. It would probably be a good idea to write a bunch of test cases, before changing it.

mawe42 commented on Mar 14, 2021 Member

Looking into `load_pgen()` some more, I think the logic behind that `hz` pointer is completely broken... and not just in the place where this PR introduces a fix. It's purpose is to be able to move a global zones that is not the first zone in a preset to the beginning of the zone list. But as `*hz` points to the local `p2` variable (i.e. the current entry in the zone list), the `preset->zone` list is not updated correctly.

mawe42 commented on Mar 14, 2021 Member

I don't see how the global zone relocation code will ever have run. As far as I understand it, the following check will always be false, because `*hz` and `p2` point to the same memory location:

fluidsynth/src/sfloader/fluid_sffile.c
Line 1517 in b8fb6c8

```
1517      if(*hz != p2)
```

And looking back through the history of this code, I arrive at the initial commit which has the same behaviour. So I guess we could either remove the relocation code altogether, or fix try to fix it.

derselbst commented on Mar 14, 2021 — Member, Author

> It's purpose is to be able to move a global zones that is not the first zone in a preset to the beginning of the zone list.

Yes, I also had the feeling it has to do with moving around zones. I also don't see how `(*hz != p2)` can ever evaluate to true.

> And looking back through the history of this code, I arrive at the initial commit which has the same behaviour

I arrived at iiwusynth: https://cvs.savannah.nongnu.org/viewvc/iiwusynth/iiwusynth/src/iiwu_defsfont.c?revision=1.1&view=markup

We could ask Peter, I'm sure he will remeber what he did 19 years ago :D

> So I guess we could either remove the relocation code altogether, or fix try to fix it.

I think we should fix it. Ideally by creating test cases. But this will take time. I would prefer to merge this and release 2.1.8 afterwards (even if it's not perfectly correct).

derselbst mentioned this pull request on Mar 14, 2021

Fix preset/instrument zone validation logic #813

Closed

mawe42 reviewed on Mar 14, 2021

View changes

`src/sfloader/fluid_sffile.c` — Show resolved

mawe42 reviewed on Mar 14, 2021

View changes

`src/sfloader/fluid_sffile.c` Outdated — Show resolved

`Update fluid_sffile.c` ✕ `6673a5f`

mawe42 commented on Mar 14, 2021 — Member

Yes, or like that :-) That should do it, at least until we cleanup this code properly.

derselbst commented on Mar 14, 2021 — Member, Author

Great! Then I will complete this tomorrow, to give **@veritas501** the chance to report back.

👍 1

derselbst merged commit **0057196** into `2.1.x` on Mar 15, 2021

16 of 19 checks passed — View details

derselbst deleted the `issue808` branch last year

jet2jet pushed a commit to jet2jet/fluidsynth-emscripten that referenced this pull request on May 27, 2021

`Invalid generators were not removed from zone list (FluidSynth#810)` ··· `0740ef5`

Reviewers

mawe42

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

2.1

Development

Successfully merging this pull request may close these issues.

None yet

3 participants