gobby / **gobby** Public

Code Issues 61 **Pull requests 1** Actions Projects Wiki ···

New issue

Jump to bottom

Fix DoS #183 #184

Merged **aburgm** merged 1 commit into `gobby:master` from `junorouse:master` on Dec 2, 2020

Conversation 9 Commits 1 Checks 0 Files changed 3

junorouse commented on Oct 4, 2020 Contributor

Print warning message when language is a NULL pointer.

aburgm requested changes on Oct 5, 2020

View changes

aburgm left a comment Contributor

If you are concerned about this, you might also want to consider handling the case of language_id being empty, which would probably lead to the same segmentation fault?

❤️ 1

`code/commands/view-commands.cpp` Outdated Show resolved

junorouse force-pushed the `master` branch from **`fc059fd`** to **`ec8f8b5`** 2 years ago Compare

junorouse requested a review from **aburgm** 2 years ago

aburgm commented on Oct 6, 2020 Contributor

I'm sorry, I just had another look at #183, and I don't believe this is a correct fix for the issue. Looking at the location of the crash (from #183), we got:

```
Thread 1 "gobby-0.5" received signal SIGSEGV, Segmentation fault.
0x000055555561d681 in Gobby::TextSessionView::set_language (this=0x0, language=language@entry=0x0) at code/core/textsessionview.cpp:429
429             gtk_source_buffer_set_language(m_buffer, language);
```

I don't think the problem is that language is NULL, but that `this` is NULL. In other words, when you make your dbus call with an existing language ID, I would still expect the application to crash, and it is the `g_assert(m_current_view != NULL)` that needs to be protected with a proper guard, not the language. A NULL language is actually valid, it just disables syntax highlighting altogether (see docs).

I'm not sure why `m_current_view` would be NULL; are you maybe making the call when there is no document open in Gobby? I think the menu item is greyed out in this case, but maybe the d-bus call can still be made. In that case I would expect many other "invalid" menu actions could be triggered that way as well, leading to similar problems.

junorouse commented on Oct 6, 2020 Contributor Author

@aburgm Sorry, I mislead the root cause of this crash.

> are you maybe making the call when there is no document open in Gobby?

- Yes.

> In that case I would expect many other "invalid" menu actions could be triggered that way as well, leading to similar problems.

So the proper solutions might be ...

1. Patch all the `g_assert` codes to print warning message instead of crashing.

```
juno@ubuntu:~/Desktop/gobby$ grep -R 'g_assert(m_current_view != NULL);' .
./code/commands/view-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/commands/edit-commands.cpp:      g_assert(m_current_view != NULL);
./code/dialogs/goto-dialog.cpp:         g_assert(m_current_view != NULL);
./code/dialogs/goto-dialog.cpp: g_assert(m_current_view != NULL);
```

2. to do nothing and maintain the current logic. (won't fix)

aburgm commented on Oct 8, 2020 Contributor

> Patch all the g_assert codes to print warning message instead of crashing.

This would be fine with me.

> to do nothing and maintain the current logic. (won't fix)

But this too. :)

👀 1

`Fix NULL dereference triggered via dbus (gobby#183)` ··· `6f34307`

junorouse force-pushed the `master` branch from `ec8f8b5` to `6f34307` 2 years ago

Compare

junorouse commented on Oct 18, 2020 Contributor Author

@aburgm I made a patch with the former one.

junorouse commented on Dec 2, 2020 Contributor Author

@aburgm ping!

aburgm merged commit `295e697` into `gobby:master` on Dec 2, 2020

---

aburgm commented on Dec 2, 2020 Contributor

Looks good to me, sorry for the delay!

❤️ 1

abergmann commented on Dec 28, 2020

CVE-2020-35450 was assigned to this issue.

This was referenced on Jan 28, 2021

Tagging a new release #188

Closed

gobby5: unstable-2018-04-03 -> unstable-2020-12-29 NixOS/nixpkgs#111107

Merged

Reviewers

aburgm ●

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants