Subject: Problem with dialogs
Posted by koldo on Mon, 14 Nov 2016 10:41:38 GMT
View Forum Message <> Reply to Message

Lately (from weeks or few months) I am having problems with dialogs. Without any apparent reason and not always, they crash the program when closing them.

For example this function called from a THISBACK after clicking a button, may crash in the destructor:

```
void ScatterCtrl::DoProcessing()
{
 ProcessingDlg(*this).Run(true);
}
```
It is also happening many times with FileSel.

It seems it happens when the dialog constructor is inside a function, like here:
```
void Function_called_by_a_THISBACK() {
 FileSel fs;
 // Do something
 // FileSel crashes in its destructor when going out of the function
}
```
Am I doing anything wrong?

Subject: Re: Problem with dialogs
Posted by mirek on Thu, 17 Nov 2016 22:52:39 GMT
View Forum Message <> Reply to Message

Please, some info. Is it trunk or 'classic'. What OS?

In trunk, I have not encountered anything like that. From what you write, it seems ok, maybe there are some special issue elsewhere?

Examples/reference crashing?

If yes, which ones?

If not, would it be possible to create some minimal example?

Subject: Re: Problem with dialogs
Posted by koldo on Fri, 18 Nov 2016 07:29:49 GMT
View Forum Message <> Reply to Message

Sorry Mirek, this problem happens randomly.

System is Windows 7 64, and I always use latest trunk.

Problem seems to disappear when dialogs are declared inside TopWindow class or are global (inside a function).

However I will follow monitoring it. Thank you.

Subject: Re: Problem with dialogs
Posted by mirek on Fri, 18 Nov 2016 07:33:07 GMT
View Forum Message <> Reply to Message

MT involved?

Subject: Re: Problem with dialogs
Posted by koldo on Mon, 21 Nov 2016 07:38:02 GMT
View Forum Message <> Reply to Message

mirek wrote on Fri, 18 November 2016 08:33MT involved?Yes, program is MT (multi threaded), although problematic dialogs do not use MT.

Subject: Re: Problem with dialogs
Posted by koldo on Tue, 29 Nov 2016 07:51:10 GMT
View Forum Message <> Reply to Message

This time the same error has appeared after calling an Exclamation().

Internally Exclamation() calls Prompt() that declares a PromptDlgWnd__ class that is destroyed when going out of Prompt() function.

The problem appears in the destructor.

File Attachments
1) Image.png, downloaded 637 times

Subject: Re: Problem with dialogs
Posted by mirek on Tue, 29 Nov 2016 09:05:40 GMT
View Forum Message <> Reply to Message

This looks like something has overwrote TopWindow instance data with garbage (icon and

largeicon members). From the description, looks like stack frame overwrite.

Any chance you are using some C arrays in your code? Or pointers to stack objects?

int h[200];

h[x] = something;

Or maybe using some library that does?

All I can say now is that I have the same setup for my major apps (win, in both 32 and 64 bit modes), I am doing a lot of stack based dialogs and prompts and never met this issue before... I do not rule out U++ as culprit, but...

Mirek

Subject: Re: Problem with dialogs
Posted by koldo on Wed, 30 Nov 2016 08:15:24 GMT
View Forum Message <> Reply to Message

Thank you Mirek, I understand. Stack overwriting could be the culprit.

Do you know if is there an easy way to check problems in the stack?

Subject: Re: Problem with dialogs
Posted by mirek on Wed, 30 Nov 2016 08:33:56 GMT
View Forum Message <> Reply to Message

koldo wrote on Wed, 30 November 2016 09:15Thank you Mirek, I understand. Stack overwriting could be the culprit.

Do you know if is there an easy way to check problems in the stack?

No easy way. I guess there are compiler options (like /GS in MSC), but never really tried them.

You can try to check all '[' (in declaration) and 'Buffer' uses. That is where I would start...

Mirek

Subject: Re: Problem with dialogs
Posted by dolik.rce on Wed, 30 Nov 2016 09:37:02 GMT

View Forum Message <> Reply to Message

koldo wrote on Wed, 30 November 2016 09:15Thank you Mirek, I understand. Stack overwriting could be the culprit.

Do you know if is there an easy way to check problems in the stack?
Hi Koldo,

You can run the code in Valgrind ;) It is slow, but can help with all kinds of invalid memory access problems. There is also some limited support in TheIDE (at least on linux).

Best regards,
Honza

Subject: Re: Problem with dialogs
Posted by koldo on Thu, 01 Dec 2016 08:03:01 GMT
View Forum Message <> Reply to Message

Thank you!

I will try both sides. Valgrind is only for Linux but there are other Windows counterparts.

The reason I imagine follows this sequence:
- A thread declares a C array
- A dialog is declared and opened
- The thread goes out of the bounds smashing dialog memory
- The dialog is closed and crashes in the destructor

This way, although both the thread and the dialog are unrelated, the thread smashes dialog memory.

It is curious that this only happens to very unrelated TopWindow subclasses. Maybe it is simply because TopWindow uses much memory and so the probability of being crashed is higher.

Subject: Re: Problem with dialogs
Posted by mirek on Thu, 01 Dec 2016 08:09:08 GMT
View Forum Message <> Reply to Message

koldo wrote on Thu, 01 December 2016 09:03Thank you!

I will try both sides. Valgrind is only for Linux but there are other Windows counterparts.

The reason I imagine follows this sequence:
- A thread declares a C array
- A dialog is declared and opened
- The thread goes out of the bounds smashing dialog memory

- The dialog is closed and crashes in the destructor

This way, although both the thread and the dialog are unrelated, the thread smashes dialog memory.

Actually, this scenario is sort of less likely: Thread has own stack, so going out of bounds there is not going to break the dialog in GUI thread (of course, you can only have dialogs in main thread's stack, but I am sure you know that).

Quote:
It is curious that this only happens to very unrelated TopWindow subclasses. Maybe it is simply because TopWindow uses much memory and so the probability of being crashed is higher.

Well, this possibly might be a reason too - you are running out of stack. Usually it ends in different error but it is worth checking: Build with verbose and check there is /STACKSIZE:8000000 or bigger number in linker.

Subject: Re: Problem with dialogs
Posted by koldo on Fri, 02 Dec 2016 07:54:18 GMT
View Forum Message <> Reply to Message

Uuups. Threads have their own stack!.

Linker has /STACK:20000000 (> 8000000)
The application is 32 bits. Exe. size in debug mode is 36 Mb.
