Subject: theIDE segmentation fault [FIXED]
Posted by masu on Sun, 27 Aug 2006 21:35:29 GMT
View Forum Message <> Reply to Message

I get a core dump when doing the following with latest UVS2 sources (608.r21):

1. start theIDE
2. open any package
3. call Help Topics
4. try to open any other package

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Sun, 27 Aug 2006 22:12:21 GMT
View Forum Message <> Reply to Message

It is much worse , it also happens if you don't do step 3.

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Sun, 27 Aug 2006 22:53:39 GMT
View Forum Message <> Reply to Message

Have you

- rebuild all

- removed theide.cfg

?

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Mon, 28 Aug 2006 18:49:10 GMT
View Forum Message <> Reply to Message

I rebuilt everything in Blitz mode and deleted cfg dir and theide.cfg.
But now it crashes after ASSIST++ has done its job.

I get the following on the console:
terminate called after throwing an instance of 'Exc'

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Mon, 28 Aug 2006 22:40:42 GMT
View Forum Message <> Reply to Message

masu wrote on Mon, 28 August 2006 14:49I rebuilt everything in Blitz mode and deleted cfg dir and theide.cfg.
But now it crashes after ASSIST++ has done its job.

I get the following on the console:
terminate called after throwing an instance of 'Exc'

Matthias

BTW, release compilation should be without blitz (results in smaller .exe). Blitz is for debug...

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Tue, 29 Aug 2006 07:50:27 GMT
View Forum Message <> Reply to Message

luzr wrote on Tue, 29 August 2006 00:40BTW, release compilation should be without blitz (results in smaller .exe). Blitz is for debug...

Yes, you are right, I remember having read that before.
But the behavior is the same without Blitz.

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Tue, 29 Aug 2006 22:03:45 GMT
View Forum Message <> Reply to Message

Strange, just compiled Linux version and everything seems to work OK.

It is possible I have fixed the bug while fixing other stuff? (Actually, that Splitter problem could be likely cause).

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Wed, 30 Aug 2006 20:31:52 GMT
View Forum Message <> Reply to Message

The problem remains even after updating to current version.
What about the console output? Do you have an idea what that means?

I observered that it crashes when Assist++ indexing takes place (at least I can see the dialog).

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Wed, 30 Aug 2006 21:08:09 GMT
View Forum Message <> Reply to Message

Yes, Exc is "standard" exception, widely used throughout U++ (in fact, String).

There is however Exc handler at the event processing active in release mode, so uncatched Exc is unlikely.

I will try again tomorrow more settings to find out what is going on. (Linux painting and clipboard need fixing too

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Wed, 30 Aug 2006 21:24:03 GMT
View Forum Message <> Reply to Message

Can I go back to a specific version with uvs2 to track down which version introduced this problem?

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Wed, 30 Aug 2006 21:34:22 GMT
View Forum Message <> Reply to Message

Versions 608-dev1 and 608.r20 are functioning and I remember that at least one 608.r21 version was functioning.
I think the error must have been introduced at the weekend (or on Friday) when I created this topic.

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Mon, 04 Sep 2006 19:24:00 GMT
View Forum Message <> Reply to Message

I have found the problem of the segfault .
The problem is the topic file uppsrc/TCtrlLib/appdoc.tpp/DlgCalc$cs-cz.tpp which when indexed in function SyncRefs (TopicBase.cpp) causes theIDE to crash on startup. After deleting this topic file theIDE starts normally.
Why? I don't know , but at least it points into a direction.

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Mon, 04 Sep 2006 19:38:06 GMT
View Forum Message <> Reply to Message

masu wrote on Mon, 04 September 2006 15:24I have found the problem of the segfault .
The problem is the topic file uppsrc/TCtrlLib/appdoc.tpp/DlgCalc$cs-cz.tpp which when indexed in function SyncRefs (TopicBase.cpp) causes theIDE to crash on startup. After deleting this topic file theIDE starts normally.
Why? I don't know , but at least it points into a direction.

Matthias

Thanks, this is promising. The topic is still in the old uncompressed format (which should work anyway), so perhaps it is conected somehow...

I was working in linux, release mode, latest version during last 3 days without problems, which made me a bit desperate while hunting this bug...

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Fri, 08 Sep 2006 07:58:53 GMT
View Forum Message <> Reply to Message

Well, I had some other things to do during last days, but I would like to resolve this soon now.

The trouble is that I am still unable to reproduce the problem.

Do you think you could do some debuging efforts? Basically, the most effective way how to debug such release problems is to put RLOGs and RDUMPs into the code to find out which code does the crash, e.g.

```
void SyncTopicFile(const String& link, const String& path)
{
RLOG(path);
 TopicInfo& ti = topic_info().GetAdd(link);
RLOG("1");
 Time tm = FileGetTime(path);
RLIG("2");
 if(ti.path == ":ide:" || ti.path == path && ti.time == tm)
  return;
 String fn = TopicCacheName(path);
RLOG("3");
 if(FileGetTime(fn) > tm) {
RLOG("4");
  ClearLinkRef(link);
RLOG("5");
....etc
```

This way you can find witch function does the crash, then repeat the process inside that function body...

Might look a bit tedious, but in fact is usually the fastest way how to debug similar release mode problems.

(BTW, I bet that at the end of process, it will be unitialized member variable

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by masu on Fri, 08 Sep 2006 10:27:00 GMT
View Forum Message <> Reply to Message

I try to track it down ...
... but before I go on holidays .

So, I can go for it after the next three weeks.

I am sorry !

Matthias

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Mon, 11 Sep 2006 14:01:27 GMT
View Forum Message <> Reply to Message

I have found it!

This is pretty weird set of circumstances...

The real error is caused by the fact that GCC by default does not allow C++ exception to go through C code (which is what new image formats do).

Now that file

uppsrc/TCtrlLib/appdoc.tpp/DlgCalc$cs-cz.tpp

is in older format which uses PNG to store images. The upgrade path for the format is to try to load all curent image formats - which throws exception (e.g. tests JPG first) through C code.

The reason I have not encountered this problem before is that the file is loaded during indexing - but I have indexing info cached on my machine, so no indexing was needed for me.

OK, the fix is to add "-fexceptions" to the build method - this enables stack unwiding of C code. To prevent further troubles, I am now adding it to the GCC builder too.

Mirek

Subject: Re: theIDE segmentation fault [BUG]
Posted by piotr5 on Thu, 21 Sep 2006 13:09:48 GMT
View Forum Message <> Reply to Message

Putting this -fexceptions as GCC-compiler options into the relevant plugin-projects does cure the abort-signal. why hasn't this solution been put into uvs? as far as I know, -fexceptions does take up more resources (with c-files only of course), and therefore shouldn't be used as a default. am I wrong?

Subject: Re: theIDE segmentation fault [BUG]
Posted by mirek on Thu, 21 Sep 2006 13:23:27 GMT
View Forum Message <> Reply to Message

[quote title=piotr5 wrote on Thu, 21 September 2006 09:09]Putting this -fexceptions as GCC-compiler options into the relevant plugin-projects does cure the abort-signal. why hasn't this solution been put into uvs?
[quote]

Well, at the moment it was put as standard into GCC builder. We do not normally export makefiles for dev versions.

Quote:

as far as I know, -fexceptions does take up more resources (with c-files only of course), and therefore shouldn't be used as a default. am I wrong?

You are right. Anyway, these resources are just in code size, not speed and they are standard for C++ code.

OTOH, I am still deciding whether to use this solution or fix image plugins not to use C++ exceptions for error handling.
