
Subject: Re: SERIOUS: Fatal error: invalid memory access

Posted by [mirek](#) on Sat, 01 Mar 2014 10:30:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

ManfredHerr wrote on Thu, 27 February 2014 10:56: Today it is a segmentation fault and I have a complete Stacktrace. It is within the appended text file.

When I noticed that there is a parameter `version=-2147483648` I remembered the comment of uninitialized variable. And indeed, in `ide.cpp` function `SetMain` there is a call of `LoadFromFile` with two parameters only. In `Stream.cpp` the function `LoadFromFile` expects three parameters, the third of which is `version`.

The compiler does not complain because `LoadFromFile` is not in any header file.

I don't know whether this is the reason but it is worth to look at.

After further analysis of posted crashdump, I was finally able to deduce what went wrong....

Thing is that `TabBar::Serialize` (at theide start) left `TabBar::Tab` attributes like `'size'` and `'pos'` uninitialized.

So on theide start, these start uninitialized, then it gets `Paint` called BEFORE having chance to initialize records by calling `Repos`.

I have fixed the issue by adding `Repos` at the end of `Serialize`, and also (just to be sure) by initializing them in the constructor.

So hopefully, both issues should be now fixed....

Mirek
