Subject: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mirek on Mon, 22 Oct 2007 16:51:21 GMT
View Forum Message <> Reply to Message

Ok, so the problem was in this function:

```
void EditorBar::InsertLines(int i, int count) {
 li.InsertN(minmax(i, 0, li.GetCount()), max(count, 0));
 if(editor->GetCheckEdited()) {
  if(editor->IsUndoOp() && li_removed.GetCount() >= count) {
   for(int t = 0; t < count; t++) {
    li.At(i + t).firstedited = li_removed[li_removed.GetCount() - count + t].firstedited;
    li[i + t].edited = li_removed[li_removed.GetCount() - count + t].edited;
   }
   li_removed.Drop(count);
   SetEdited(i + count, 1);
   ignored_next_edit = true;
  }
  else {
   if (li[i].firstedited == 0)
    li[i].firstedited = li.At(i + count).firstedited;
   SetEdited(i + 1, count);
  }
 }
 Refresh();
}
```

Quiz: Where is the bug?

Just to make it easier: It is a very ugly catch that Upp::Vector shares with std::vector .... and with MSC it works...

Mirek

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mdelfede on Tue, 23 Oct 2007 13:11:31 GMT
View Forum Message <> Reply to Message

Very VERY happy about that... It works !

But.... where was the bug ?

Ciao

Max

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mirek on Tue, 23 Oct 2007 14:52:48 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Tue, 23 October 2007 09:11Very VERY happy about that... It works !

But.... where was the bug ?

Ciao

Max

On this line:

```
li[i].firstedited = li.At(i + count).firstedited;
```

Mirek

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mdelfede on Tue, 23 Oct 2007 15:31:34 GMT
View Forum Message <> Reply to Message

luzr wrote on Tue, 23 October 2007 16:52
On this line:

```
li[i].firstedited = li.At(i + count).firstedited;
```

I suppose the operator [] uses a static temporary or something like that ?

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mirek on Tue, 23 Oct 2007 15:41:32 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Tue, 23 October 2007 11:31luzr wrote on Tue, 23 October 2007 16:52

On this line:

```
li[i].firstedited = li.At(i + count).firstedited;
```

I suppose the operator [] uses a static temporary or something like that ?

Nope. But it returns a reference. However, .At invalidates references to Vector.... So if the left side of statement is evaluated before the right side, you have "free block overwrite"...

Mirek

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mdelfede on Tue, 23 Oct 2007 15:50:12 GMT
View Forum Message <> Reply to Message

luzr wrote on Tue, 23 October 2007 17:41

Nope. But it returns a reference. However, .At invalidates references to Vector.... So if the left side of statement is evaluated before the right side, you have "free block overwrite"...

Mirek

Uhmmm... what is the reason of invalidating the ref ? At() isn't the same as operator [], for array ? The only reason to invalidate the ref I could imagine is that At() (can) make a deep copy of array...

BTW, I was thinkin' about it yesterday.... why did you use the pick_ stuff instead of something like a pimpl object with copy-on-write ? It's not feasible ?

Ciao

Max

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mirek on Tue, 23 Oct 2007 16:08:41 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Tue, 23 October 2007 11:50luzr wrote on Tue, 23 October 2007 17:41

Nope. But it returns a reference. However, .At invalidates references to Vector.... So if the left side

of statement is evaluated before the right side, you have "free block overwrite"...

Mirek

Uhmmm... what is the reason of invalidating the ref ? At() isn't the same as operator [], for array ?

No, it can resize the array if you use i >= GetCount.

Quote:
BTW, I was thinkin' about it yesterday.... why did you use the pick_ stuff instead of something like a pimpl object with copy-on-write ? It's not feasible ?

IMO/IME, shared ownership is the root of evil At least in C++.

Mirek

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mdelfede on Tue, 23 Oct 2007 16:20:15 GMT
View Forum Message <> Reply to Message

luzr wrote on Tue, 23 October 2007 18:08
No, it can resize the array if you use i >= GetCount.

Ah, ok... I wouldn't ever use it like that, it's the easy way of producing bugs.... Much better an explicit Realloc() or something like that. BTW resizing the array makes the assumption that elements have a default constructor, too.

Quote:
IMO/IME, shared ownership is the root of evil At least in C++.

well, if you share ownership (like I've suggested) you MUST avoid any kind of pointers, but if it's well done can be rock solid.
Of course, if you use reference counted stuffs and than you take address of if, you can be sure about having bugs

I must say that reference counted stuffs are usually small in size, so you can pass them by value with few overhead.
I did something like that some time ago and it was nice to use.

Ciao

Max

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mirek on Tue, 23 Oct 2007 17:45:20 GMT
View Forum Message <> Reply to Message

mdelfede wrote on Tue, 23 October 2007 12:20luzr wrote on Tue, 23 October 2007 18:08
No, it can resize the array if you use i >= GetCount.

Ah, ok... I wouldn't ever use it like that, it's the easy way of producing bugs....

Well, I think At is extremely effective way how to solve many problems. And similar issue existis even in the plain C

a[i++] = a[i];

it is simply something you have to care about...

Quote:
I must say that reference counted stuffs are usually small in size, so you can pass them by value with few overhead.
I did something like that some time ago and it was nice to use.

Well, yes, I think that is the "official" C++/boost path... If you like that, U++ pick_ must sound alien to you

Mirek

Subject: Re: Hopefully fixed "Writes to freed blocks" bug in ide - and warning (quiz)
Posted by mdelfede on Tue, 23 Oct 2007 19:47:30 GMT
View Forum Message <> Reply to Message

luzr wrote on Tue, 23 October 2007 19:45
Well, I think At is extremely effective way how to solve many problems. And similar issue existis even in the plain C

a[i++] = a[i];

it is simply something you have to care about...

Well, in your example, you can see that you're doing it wrong.
In theide bug, you can't.... or, at least, you can't if you don't know upp vector internals, what's normally the matter.
Usually people see Vector<> as a blackbox, they don't know (at least, I didn't know) about invalid references caused by At().

OTOH, people that program in C++ usually know that A[i++]=A[i] is a nonsense.

Quote:
Well, yes, I think that is the "official" C++/boost path... If you like that, U++ pick_ must sound alien to you

Uhm... I don't know Boost++ in depth, but I don't think PIMPL+reference counting is their base path.
I know that reference counting + pointers is an hassle, but together with PIMPL and WITHOUT use of pointers can be quite good. That said, I don't like too much Boost++, I find it well written but old style coding. I did write my own Array class in past because of that.
BTW, I still think that c++ standard is missing many useful constructs, one of the most useful ot them is the 'property' one, which borland introduced as a language extension in their compilers. An object-oriented language without properties is an empty wine glass, I think

Just an example of it :

```
class C
{
  private:

  int iVal;

  void set_iVal(int _i) { i = _iVal; }
  int get_iVal(void) { return iVal; }

  public:

  __property i = { read = getIval, write = setIval };

};

C c ;

c.i = 5;  // calls set_Ival(5)
int a = c.i; // calls a = get_Ival()
```

That's what I call 'clean object-oriented language'.

Ciao

Max