Subject: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mirek on Wed, 14 May 2008 11:14:47 GMT
View Forum Message <> Reply to Message

I was hunting this one for about 12 hours total, tracked the problem down, seen the broken assembly and prepared the isolated test.

This test should print "32", which is the sizeof(Item). But if you compile it with -O3 flag under

gcc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu7)

it prints 0.

Please check, maybe there is still something wrong with code, some undefined behaviour:

CGGBug.h

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <new>

template <class T> inline const T& my_max(const T& a, const T& b) { return a > b ? a : b; }
template <class T> inline const T& my_min(const T& a, const T& b) { return a < b ? a : b; }

template <class T>
inline T minmax(T x, T _min, T _max) { return my_min(my_max(x, _min), _max); }

void *MemoryAllocSz(size_t& sz);
void  MemoryFree(void *);

template <class T>
class Vector {
 T       *vector;
 int      items;
 int      alloc;

 static void RawFree(T *ptr)            { if(ptr) MemoryFree(ptr); }
 static T   *RawAlloc(int& n);

 void RawInsert(int q, int count);


public:
 void  InsertN(int q, int count);
 const T& First() { return vector[0]; }
 int   GetCount() const { return items; }
 Vector() { vector = NULL; items = alloc = 0; }
};

template <class T>
T * Vector<T>::RawAlloc(int& n)
{
 size_t sz0 = n * sizeof(T);
 size_t sz = sz0;
 void *q = MemoryAllocSz(sz);
 n += (int)((sz - sz0) / sizeof(T));
 return (T *)q;
}

template <class T>
void Vector<T>::RawInsert(int q, int count)
{
 if(!count) return;
 if(items + count > alloc) {
  T *newvector = RawAlloc(alloc = alloc + my_max(alloc, count));
  if(vector) {
   memcpy(newvector, vector, q * sizeof(T));
   memcpy(newvector + q + count, vector + q, (items - q) * sizeof(T));
   RawFree(vector);
  }
  vector = newvector;
 }
 else {
  memmove(vector + q + count, vector + q, (items - q) * sizeof(T));
 }
 items += count;
}

template <class T>
void Vector<T>::InsertN(int q, int count)
{
 RawInsert(q, count);
}

void *MemoryAllocSz(size_t& sz);
void  MemoryFree(void *);

struct Item {
 char h[32];
};

struct Bar {
 Vector<Item> li;
 void DoTest(int i, int count);
};
```

GCCBug1.cpp

```
#include "GCCBug.h"

char array[256];

void *MemoryAllocSz(size_t& sz)
{
 printf("%d\n", sz);
 return array;
}

void MemoryFree(void *) {}
```

GCCBug2.cpp

```
#include "GCCBug.h"

void Bar::DoTest(int i, int count)
{
 li.InsertN(minmax(i, 0, li.GetCount()), my_max(count, 0));
}
```

GCCBug3.cpp

```
#include "GCCBug.h"

int main(int argc, char argv[])
{
 Bar b;
 b.DoTest(0, 1);
 return 0;
}
```

(Note, it is probably important to keep all this in 4 specific files to avoid specific inlining variants).

Compiled with flags:

```
-ggdb -g2  -fexceptions  -O3 -x c++
```

Mirek

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mdelfede on Wed, 14 May 2008 22:14:49 GMT
View Forum Message <> Reply to Message

confirmed. After rebuild with gcc-4.1 all memory violations went away and theide become stable as used to be in ubuntu feisty.

Ciao

Max

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mr_ped on Thu, 15 May 2008 08:54:46 GMT
View Forum Message <> Reply to Message

So is this reported to GCC team or at least to Ubuntu so they can push upstream a bit?
I think this is quite critical, I will probably search trough launchpad (ubuntu bug+stuff system) today to see if it is reported and if not, I will report it.

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mirek on Thu, 15 May 2008 11:12:27 GMT
View Forum Message <> Reply to Message

GCC yes.

Ubuntu not. I would be glad if you would do it.

Mirek

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mr_ped on Thu, 15 May 2008 11:16:27 GMT
View Forum Message <> Reply to Message

Can you post here some URL to GCC bug report, so it's easy for everyone from this forum to track it? I'm really lazy today.

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mdelfede on Thu, 15 May 2008 11:47:49 GMT
View Forum Message <> Reply to Message

http://gcc.gnu.org/bugzilla/show_bug.cgi?id=36235

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mr_ped on Thu, 15 May 2008 12:28:49 GMT
View Forum Message <> Reply to Message

Reported to launchpad too, but I'm afraid they will not change the GCC version in 8.04.
https://bugs.launchpad.net/gcc/+bug/230682

Anyway, the 4.2 is already uploaded into Intrepid too (next Ubuntu 8.10 release), so I hope they will move to 4.3 ASAP at least there.
Although till it's release date there will be maybe yet another "current" version of gcc.

Let's see.

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by bytefield on Thu, 15 May 2008 15:17:18 GMT
View Forum Message <> Reply to Message

Edit: (compiler confusion)

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by cocob on Wed, 21 May 2008 20:30:35 GMT
View Forum Message <> Reply to Message

I'am using debian testing with 2007.1. My g++ version is 4.2.3 and i have no problems with U++. Normal or not ?

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mdelfede on Wed, 21 May 2008 21:47:24 GMT
View Forum Message <> Reply to Message

cocob wrote on Wed, 21 May 2008 22:30I'am using debian testing with 2007.1. My g++ version is 4.2.3 and i have no problems with U++. Normal or not ?

It depends... If you use 2007.1 binary, which is compiled against GCC 4.1 or earlier, you won't have problems RUNNING theide, but compiling against GCC 4.2.3 you've got a good chance to have problems with your compiled apps.
More, if you don't enable -O3 optimization (or, better said, -finlune-functions optimization, which is in -O3), you shouldn't have problems.

Ciao

Max

Subject: Re: Recent Ubuntu8.04 troubles confirmed to be the compiler bug
Posted by mr_ped on Thu, 22 May 2008 07:37:38 GMT

View Forum Message <> Reply to Message

From gcc bug: "4.2.4 is being released, changing milestones to 4.2.5."