

Re: VC 2003, WinXP and Win2000

Source: <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.language/2006-06/msg00495.html>

- *From:* "Doug Harrison [MVP]" <dsh@xxxxxxxx>
 - *Date:* Wed, 14 Jun 2006 11:03:14 -0500
-

On 14 Jun 2006 08:21:15 -0700, "TemporalBeing" <gpclock@xxxxxxxx> wrote:

I was recently forced to upgrade from Win2k SP4 to WinXP SP1, and this issue does not seem to occur at all under Win2k SP4.

I am working with the wincrypt, and allocating a buffer to hold some data. This is done numerous times in the code, but only fails on the last one. The code flow is basically allocate, copy, allocate, copy until all data in a buffer used by wincrypt is extracted into separate buffers.

The problem I am running into is that the memcpy is generating a first-chance exception under WinXP. (This does not happen at all under Win2k.) If I run the program on the command-line then the program works fine – the first-chance exception is still generated but silently ignored and the program works as expected (passing my unit tests). The problem I am running into is that I have a unit test later in the program that I am trying to debug, but I cannot get to it via the debugger because of this first chance exception.

This suggests you're having the debugger stop on all exceptions, including "first chance" ones, which can be ignored most of the time:

First and second chance exception handling
<http://www.support.microsoft.com/kb/105675>

The code is basically the following:

```
BYTE* pointer_into_wincrypt_buffer;
// Ex: 512 bits / 8 bits [per byte] = 64 bytes
data_size = key_bit_length / 8;
...
void* Data = malloc(data_size);
memset(Data,0,data_size);
memcpy(Data,pointer_into_wincrypt_buffer,data_size);
```

Re: VC 2003, WinXP and Win2000

So far as I can tell, the buffer sizes are correct. In looking online, I came across one post that suggested this issue could be caused by the compiler interpreting the data wrong, so I also tried changing the memcpsy() line to the following:

```
memcpy((BYTE*)Data,pointer_into_wincrypt_buffer,data_size);
```

However, I still have the same problem. I have also tried changing Data from being a void* to an unsigned char*, but it did not resolve the issue.

As memcpy takes a void* and operates internally on bytes, that should have no effect.

As I said earlier, I do this a number of times and it only does this on the last one. The code is correct, but I can't get the debugger to go past it.

What are the values of Data and data_size the last time around?

Debugger error is 0xC0000005 (invalid pointer) and occurs on the 'rep movsd' in memcpy. Ignore is disabled. I would be more greatly concerned if it was also occurring under Win2k, but I cannot find any reason why it would under WinXP and not under Win2k, and why it would work correctly when run under the debugger if there really was an issue.

Any ideas/tips/etc greatly appreciated.

You should not be getting an exception, and it's worrisome that it's being handled, as it ought to be causing your program to crash. Concerning the Win2K/WinXP discrepancy, differences in heap management could account for that. I suspect a bug either in your code or memcpy, especially if you're using the intrinsic form. To rule out a memcpy codegen bug, try writing your own version, give it a different name, and drop it in as a temporary replacement. You could replace it with std::copy if you're using the C++ Standard Library.

--

Doug Harrison
Visual C++ MVP

.