Subject: Re: Optimized memcmp for x86
Posted by mr_ped on Sat, 23 Feb 2008 22:23:01 GMT
View Forum Message <> Reply to Message

cbpporter wrote on Sat, 23 February 2008 22:18Quote:Than again if such OS allocators allow to allocate only for example 4kB chunks and not 13 bytes, I think it will never raise exception or crash and you may safely read beyond end of buffer.
That is true, but it will not allocate those 4KB for every 13 bytes you want, only if the previoslly allocated 4KB chunk is full. Your requested pointer may be on the end of that allocated zone, and here you could have big problems.

Anyway, this is a memcmp operation, so even if you don't crash, just getting gibberish data could compromise the functionality.

If you get truly 13B from end of 4kB chunk, the starting address will be not aligned => classic memcmp will be called.

If starting pointer is aligned and you know the whole 4kB chunk is readable, you may safely read 4bytes even if the last 3 are beyond the original buffer, you can't cross 4kB chunk boundary in any case.

Those gibberish data are masked out before comparison.
You should probably check the original routine and my suggestion firstly to get idea what's the problem with that last double word read from memory.