Can memcpy go into an infinite loop? Why is it being blamed for a busy hang?

devblogs.microsoft.com/oldnewthing/20170413-00

April 13, 2017

Raymond Chen

A customer reported that their program locks up once or twice each day. They took a full dump of the file while it was hung and asked `windbg` to analyze it. Here's a redacted version of what it said:

```
PRIMARY_PROBLEM_CLASS: APPLICATION_HANG_BusyHang

STACK_TEXT:
msvcr80!_memcpy+0x7d
contoso!Buffer::Compact+0x3d
contoso!BufferReader::Parse+0x14c
contoso!handle_widget_message+0x37
contoso!handle_input+0x12f
contoso!dispatch_event+0x27
contoso!handle_events+0xbe
```

The `Buffer::Compact` method shifts some memory around inside the buffer:

```
void Buffer::Compact()
{
  if (m_bytesRead > 0) {
    memmove(m_buffer, m_buffer + m_bytesRead, m_capacity - m_bytesRead);
    m_capacity -= m_bytesRead;
    m_bytesRead = 0;
  }
}
```

"Is it possible that `memmove` has a busy wait? What could it be waiting for?"

The `memmove` function doesn't have a busy loop where it waits for something. It just moves the memory from one location to another.

What's probably happening is that there is a busy loop higher up the stack. Maybe `Buffer-Reader::Parse` has gotten into a loop, or (my guess) `handle_events` is stuck in a loop processing a huge number of incoming events.

When you take the memory dump, you are capturing the program at a moment in time. All you know is that the thread is probably in a busy wait, but the source of the busy wait need not be the thing at the top of the stack.

If `memcpy` is consistently at the top of the stack, then it means that the thread is spending most of its time copying memory. But that doesn't necessarily mean that `memcpy` is stuck in a loop. The more likely reason is that the thread is busy doing some larger operation, and that larger operation entails a lot of `memcpy` operations.

Though in extreme edge cases it might be a busy loop.

Sort-of related.

Exercise: The customer's code calls `memmove`, so why is the `memcpy` function the one at the top of the stack? What happened to `memmove`?

Raymond Chen

Follow