

Re: _sprintf

Source: <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2006-08/msg00439.html>

- *From:* Joseph M. Newcomer <newcomer@xxxxxxxxxxxxx>
 - *Date:* Mon, 31 Jul 2006 16:30:22 -0400
-

The libraries are shared and there is already a copy of them loaded.

What is wrong with StringCchPrintf? It won't overflow the buffer, which is a good thing.

The char/wchar_t is what TCHAR means. But it is signed, which implies sign extension for any Unicode character > 7FFFU. This will not produce a good result in most cases. WORD will handle a char value because it won't sign extended.

I made B an array of two characters. not two bytes. I distinctly recall writing
TCHAR B[2];
which is two characters. This means in Unicode it is 4 bytes.

StringCchPrintf will format the string, which is one character plus a terminal null character. Do not confuse "character" with "byte". StringCchPrintf will copy the single character and add a NULL character, which the last I looked, was two characters, the size of the array.
joe

On Mon, 31 Jul 2006 19:40:24 +0900, "Norman Diamond" <ndiamond@xxxxxxxxxxxxxxxxx> wrote:

"Joseph M. Newcomer" <newcomer@xxxxxxxxxxxxx> wrote in message
news:e57oc2lrr2nd1j0nt83h8e7h02ahjsbqih@xxxxxxxxxxxxx

Use CString::Format as the preferred choice.

On "real" Windows I agree. On Windows CE where extra libraries will occupy the machine's RAM, it might not be a good idea.

If you MUST use some form like _sprintf, use StringCchPrintf (I think that's the name, but search for strsafe.h on the MSDN) which at least will avoid any possibility of buffer overflow

As documented it will not have such a beneficial effect.

Re: _stprintf

```
StringCchPrintf(_T("%c"), B, sizeof(B) / sizeof(TCHAR), (BYTE>('a' + i));
```

Mihai N. addressed a problem with your cast to BYTE and you made an adjustment which I'm still thinking about. Since arguments to StringCchPrintf are either Unicode or ANSI, the last argument should be either char or wchar_t, and I'm trying to figure out if WORD is guaranteed to marshall a char value properly.

More importantly is that, as documented, buffer overflow can very easily occur. Suppose we have an ANSI compilation and make B an array of 2 chars. Then the buffer has enough space for 1 single-byte character plus a null character. But if the last argument is a double-byte character then StringCchPrintf is documented to copy both bytes plus a single-byte null character, total 3 bytes.

Joseph M. Newcomer [MVP]

email: newcomer@xxxxxxxxxxxx

Web: <http://www.flounder.com>

MVP Tips: http://www.flounder.com/mvp_tips.htm

.