

Re: Memory leak

Source:

<http://www.tech-archive.net/Archive/WindowsCE/microsoft.public.windowsce.embedded.vc/2004-02/0589.html>

From: Michael J. Salamone [eMVP] (*mikesa#at#entrek#dot#com*)

Date: 02/26/04

Date: Thu, 26 Feb 2004 04:40:01 -0800

I haven't looked thoroughly through your code snippet, but the biggest thing that worries me is the potential for memory overwrites (memory corruption).

For example, in these line:

```
> strncpy(m_XMLMessage,(const char*) XML, strlen(XML)+1);
```

Is it possible XML string is larger than m_XMLMessage buffer will accomodate? You probably want 1024, or better, sizeof(m_XMLMessage), instead of strlen(XML)+1.

```
> m_XMLMessage[strlen(m_XMLMessage) + 1] = '\0';
```

The available subscripts on a string, just like any array, are 0..n, where n=size of the array (in chars, or elements) - 1.

In your case, you can go from 0-1023. And the max NULL-terminated string you could have is 1023 characters plus a NULL terminator - 1024 characters total.

If, in your case, the string was exactly the number of characters you could have (1023), then strlen(m_XMLMessage) is 1023, that + 1 is 1024, and you have corruption. You don't want the "+1".

You also have calls to mbstowcs and wbstombs that I see "+1"'s in. Again I didn't go through this thoroughly, but I'm betting that's your problem.

Btw, you probably don't want a number like "60" in your code. You should probably have a sizeof() or #define or just about anything other than 60. I see you declared your buffer that long, but I'm most worried about the call to wbstombs that uses it. As soon as you change that 60 to something smaller, you're toast. You sizeof(m_CommandType).

Why do you assume a leak?

Also, I would review all my code for similar problems.

--

Michael Salamone [eMVP]

Re: Memory leak

microsoft.public.windowsce.embedded.vc: Re: Memory leak

Entrek Software, Inc.

www.entrek.com

"Siv" <anonymous@discussions.microsoft.com> wrote in message
news:22b901c3fc56\$3d4d77e0\$a401280a@phx.gbl...

> Hi,

>

> There is a a memory leak in a application, and i think
> the leak is caused by the following function, which is
> called in the main application many times(in while a
> loop). Moreover after running the application for 15min
> the following function fails. Below is the function. Can
> anyone spot a memory leak in the function???

>

> //////////////////////////////////////

> //////////////////////////////////////

> //Returns tag value for a given tag name from XML event
> notification

> //IN tag name

> //return tag value

> char* GetTagValueFromXMLmessage(char* XML,char* tagName)

> {

>

>

> char m_XMLMessage[1024];

> strncpy(m_XMLMessage,(const char*) XML, strlen(XML)+1);

> m_XMLMessage[strlen(m_XMLMessage) + 1] = '\0';

>

> char m_tagName[100];

> strncpy(m_tagName,(const char*)tagName,strlen(tagName)+1);

> m_tagName[strlen(m_tagName) + 1] = '\0';

>

> IXMLDOMDocument *iXMLDoc = NULL;

> IXMLDOMNodeList *iXMLNodeList = NULL;

> IXMLDOMNode *iXMLNodeCommandPtr = NULL;

>

> HRESULT hr;

> VARIANT_BOOL tEmpty;

>

> BSTR bstrCommandText;

> wchar_t pwc_xml[sizeof(wchar_t)*1024];

> wchar_t pwc_tagName[sizeof(wchar_t)*100];

>

> char m_xml[1024];

> char m_CommandType[60];

>

> _try

> {

>

> //create instance of msXML COM componenet

> hr = CoInitializeEx(NULL,COINIT_MULTITHREADED);

> if(!SUCCEEDED(hr)) return 0;

>

> hr = CoCreateInstance (CLSID_DOMDocument, NULL,

> CLSCTX_INPROC_SERVER | CLSCTX_LOCAL_SERVER,

> IID_IXMLDOMDocument,(LPVOID *)&iXMLDoc);

>

> if(iXMLDoc)

> {

> iXMLDoc->put_async(VARIANT_FALSE);

>

> //convert xmlMessage to wchar

> int ii = mbstowcs(pwc_xml, m_XMLMessage, strlen

microsoft.public.windowsce.embedded.vc: Re: Memory leak

```
> (m_XMLMessage) + 1 );
>
>
> //Load XML
> iXMLDoc->loadXML( pwc_xml, &tEmpty);
>
>
> //convert tagName to wchar
> ii = mbstowcs( pwc_tagName,m_tagName, strlen(m_tagName)
> +1 );
>
> //get command node
> //iXMLDoc->getElementsByTagName(L"Value",&iXMLNodeList);
> iXMLDoc->getElementsByTagName(pwc_tagName,&iXMLNodeList);
>
> iXMLNodeList->get_item(0, &iXMLNodeCommandPtr);
>
> iXMLNodeCommandPtr->get_text(&bstrCommandText);
> ii = wcstombs( m_CommandType, bstrCommandText, 60 );
>
> }//end if
>
> //Release memory
> iXMLNodeList->Release();
> iXMLNodeList = NULL;
> iXMLNodeCommandPtr->Release();
> iXMLNodeCommandPtr = NULL;
> iXMLDoc->Release();
> SysFreeString(bstrCommandText);
>
>
>
> }
> __except(EXCEPTION_EXECUTE_HANDLER)
> { int di;
> printf("ERROR in ..XML parse for tag: %
> s\n",m_tagName);
> scanf("%d",&di);
>
> }
>
> char a_m_xml[1024];
> strncpy(a_m_xml,m_CommandType, strlen(m_CommandType)
> +1);
>
> return a_m_xml;
>
>
>
> }
>
> Any replies is much appreciated
>
> Thanks
> Siv
```