

Re: Who could tell me why the error address isn't the same?

Re: Who could tell me why the error address isn't the same?

Source: <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2007-02/msg01218.html>

- *From:* Mihajlo Cvetanovic <mac@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 14 Feb 2007 12:36:38 +0100
-

"Lee Tow" <fbjlt@xxxxxxxxxxxxx> wrote in message
[news:e%23ttv8\\$THHA.5060@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e%23ttv8$THHA.5060@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hello all:

Look:

```
char str[]="ABCDEFGHJKLMNOPQRSTUVWXYZ";  
void main()  
{  
char name[8];  
strcpy(name,str);  
}
```

I use vc6.0,and when I set active project configuration to Win32 Debug,and then the error address is 0x504f4e4d,and I set active project configuration to Win32 Release and the error address is 0x4c4b4a49,I want to know why error addresses are different in the same codes?Thanks very much.

If you look carefully at those "addresses" you'll notice that they have the same pattern. They're comprised of the letters from original <str>. 0x504f4e4d is the substring "MNOP", and 0x4c4b4a49 is the substring "IJKL". What actually happened is that the strcpy was writing outside of the memory occupied by <name> (which is a bug), into the rest of the stack. One place in the stack is used to tell the function (main) where to return to when it's done, and this place was overwritten with "MNOP" and "IJKL". So when the <main> tries to "return", it actually tries to jump to memory location "MNOP", which is unaccessible (luckily for you, because you've found the bug).

The difference between Debug and Release is that Debug build puts some extra data on the stack to help you debug easily. Because of this extra data the rest of the stack in Debug build is spoiled with garbage by 4 byte offset (in regards to Release build).