查看: 1656 | 回复: 20

【讨论】关于返回C语言局部指针变量的有趣&奇怪问题 [复制链接]

VBProFan

版主

擂点 3
人气 1235
威望 3030
注册时间 2006-6-14
精华 9
帖子 13571

串个门 加好友
打招呼 发消息

发表于 2010-5-25 17:33:06 | 只看该作者 | 倒序浏览 1楼 电梯直达

在 VC6 里编译如下代码:

```
#include <stdio.h>
char *GetString(void)
{
    char p[] = "ABCDE";
    return p;    // 如果用p[]编译器将提出警告
}
void main()
{
    printf("%s\n", GetString());
}
```

复制代码

编译时出现警告，运行结果输出乱码。
然后把char p[] = "ABCDE"; 改为 char *p = "ABCDE";
编译时不再出现警告，运行结果也正常。这是为什么？
请自己思考一下再看下面的答案（白字）：

然而奇怪的是，我在 VC6 里跟踪p[]版本的汇编代码，如下：

```
13:       printf("%s\n", GetString());
00401098  call      @ILT+5(GetString) (0040100a)
0040109D  push      eax
0040109E  push      offset string "%s\n" (00422024)
004010A3  call      printf (00401130)
```

先把 printf 的两个参数入栈再调用它。在入栈后调用前我查看了一下eax指向的内存单元，发现还是 ABCDE，按理说输出也应该是 ABCDE，可是为什么是乱码呢？如果是乱码的话，那应该是退出了 GetString 函数后局部数据区（堆栈）马上被这些乱码覆盖才对，可是并没有被乱码覆盖。
然后我又怀疑是不是 VC6 的内存显示窗口没有及时根据内存中的内容来刷新显示，于是又试了一下 OllyDbg，结果依旧。
神奇了。。。哪位大侠来指点一下迷津？

请稍候...

使用道具 举报

msflexgrid

高级程序员

播点	0
人气	78
威望	52
注册时间	2009-4-30
精华	0
帖子	1260

串个门 加好友 打招呼 发消息

发表于 2010-5-25 18:51:06 | 只看该作者 2楼

VC2008编译器提示局部或临时变量

warning C4172: returning address of local variable or temporary

1

查看全部评分 VBProFan

SIGNATURE

你们懂的...

举报

msflexgrid

高级程序员

播点	0
人气	78
威望	52
注册时间	2009-4-30
精华	0
帖子	1260

串个门 加好友 打招呼 发消息

发表于 2010-5-25 19:03:11 | 只看该作者 3楼

因为char p[] = "ABCDE";在函数体内
所以退出后这个空间不再保留了
进入printf之前空间还在内存中残留，
进入printf后，被printf的push指令压入的数据覆盖了.....所以最后显示乱码

附件: 你需要登录才可以下载或查看附件。没有帐号？注册

1

查看全部评分 VBProFan

SIGNATURE

你们懂的...

举报

msflexgrid

发表于 2010-5-25 19:12:00 | 只看该作者 4楼

压入的是那个printf变长参数的结束标志 －1

```
int __cdecl printf (
        const char *format,
        ...
        )
/*
* stdout 'PRINT', 'F'ormatted
```

高级程序员

擂点	0
人气	78
威望	52
注册时间	2009-4-30
精华	0
帖子	1260

串个门 加好友
打招呼 发消息

```
*/
{
        va_list arglist;
        int buffing;
        int retval;

        _VALIDATE_RETURN( (format != NULL), EINVAL, -1);
```

SIGNATURE

你们懂的...

举报

VBProFan

发表于 2010-5-25 20:10:08 | 只看该作者 5楼

试验了一下，确实要进入 printf 内部才会覆盖“ABCDE”所在的内存区。而 *p 版本的“ABCDE”所在的内存区的地址明显比较大，是全局数据区，所以进入后也不被覆盖。而且输出的“乱码”和原地址的数据相符（对比ASCII字符表，类C、空格、上下箭头）。

但还有个遗留问题没想明白，跟踪 printf，发现输出字符到控制台的是这一句：
0040119A call _ftbuf (004014e0)
在这句执行前手工设置对应的内存区为“HIJ”，但输出的结果还是那三个“乱码”.....

版主

擂点	3
人气	1235
威望	3030
注册时间	2006-6-14
精华	9
帖子	13571

串个门 加好友
打招呼 发消息

SIGNATURE

请稍候...

举报

VBProFan

发表于 2010-5-25 20:29:39 | 只看该作者 6楼

> 压入的是那个printf变长参数的结束标志 −1
>
> ```
> int __cdecl printf (
>         const char *format,
>         ...
>         )
> /*
> * stdout 'PRINT', 'F'ormatted
> */
> {
>         va_list arglist;
>         i ...
> ```
>
> msflexgrid 发表于 2010-5-25 19:12

版主

擂点	3
人气	1235
威望	3030
注册时间	2006-6-14
精华	9
帖子	13571

串个门 加好友
打招呼 发消息

呵呵，原来 printf 也是用结束标志来处理变长参数的。如果有个变长参数的函数可接受任意数据类型，就不知道它怎么判断结束了。

SIGNATURE

请稍候...

举报

ichanging

初级程序员

擂点	0
人气	1
威望	0
注册时间	2010-5-25
精华	0
帖子	1

串个门 加好友
打招呼 发消息

发表于 2010-5-25 22:31:49 | 只看该作者 7楼

泡饭
我5点20告诉你答案，你5点33就发帖了？

1

查看全部评分

VBProFan

举报

VBProFan

版主

擂点	3
人气	1235
威望	3030
注册时间	2006-6-14
精华	9
帖子	13571

串个门 加好友
打招呼 发消息

发表于 2010-5-26 10:16:20 | 只看该作者 8楼

成功

本帖最后由 VBProFan 于 2010-5-26 10:43 编辑

注意，修改后在 ret 前的 pop ebp 之前要记得改回“80 FF 12 00”；另外，要在
00401186 call _output (004015a0)
前修改数据区才行，如果运行了这句 call 再修改，输出的仍然是原来的乱码。

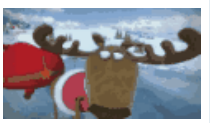
附件: 你需要登录才可以下载或查看附件。没有帐号？注册

SIGNATURE

请稍候...

举报

acme_pjz



系统设计师
最大自定义头衔长度半

发表于 2010-5-26 11:23:32 | 只看该作者 9楼

泡饭你这个代码写得很不严谨啊.....虽然返回结果是对的，但是指不定什么时候就出莫名其妙的错误了.....

相对标准一点的写法是:

```
#include <stdio.h>
char *GetString(void)
```

个量子比特

播点 11
人气 1219
威望 2446
注册时间 2005-7-23
精华 6
帖子 17151

串个门 加好友
打招呼 发消息

```
{
    static char p[最好指定一个大小] = "ABCDE";
    return p;
}
void main()
{
    printf("%s\n", GetString());
}
```

SIGNATURE

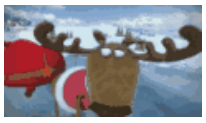
本人使用半个操作系统，至于你信不信，我反正信了

谷歌代码开源项目:摇方块/摇立体 山寨编译器

囧，签名超长了

举报

acme_pjz



系统设计师

最大自定义头衔长度半个量子比特

播点 11
人气 1219
威望 2446
注册时间 2005-7-23
精华 6
帖子 17151

串个门 加好友
打招呼 发消息

发表于 2010-5-26 11:25:02 | 只看该作者 10楼

当然最简单的写法是:

```
char *GetString(void)
{
    return "ABCDE";
}
```

可能会提示常指针错误.....这样的话就改成const char* XXX.....

SIGNATURE

本人使用半个操作系统，至于你信不信，我反正信了

谷歌代码开源项目:摇方块/摇立体 山寨编译器

囧，签名超长了

举报

发帖

返回列表 1 2 3 下一页

高级模式

您需要登录后才可以回帖 登录 | 注册

replysubmit 回帖后跳转到最后一页