BOOL WriteProcessMemory(

HANDLE hProcess,

LPVOID lpBaseAddress,

LPVOID lpBuffer,

DWORD nSize,

LPDWORD lpNumberOfBytesWritten

);

参数:

hProcess

由[OpenProcess](http://baike.so.com/doc/6840318-7057593.html" \t "http://baike.so.com/doc/_blank)返回的进程句柄。

如参数传数据为 INVALID\_HANDLE\_VALUE 【即-1】目标进程为自身进程

lpBaseAddress

要写的内存首地址

再写入之前，此[函数](http://baike.so.com/doc/5368923-5604762.html" \t "http://baike.so.com/doc/_blank)将先检查目标地址是否可用，并能容纳待写入的数据。

lpBuffer

指向要写的数据的[指针](http://baike.so.com/doc/1043844-1104112.html" \t "http://baike.so.com/doc/_blank)。

nSize

要写入的字节数。

返回值

非零值代表成功。

可用[GetLastError](http://baike.so.com/doc/6950177-7172578.html" \t "http://baike.so.com/doc/_blank)获取更多的错误详细信息。

所在头文件: Winbase.h

链接库: Nk.lib

例：

//将DLL的路径名复制到远程进程的内存空间

if (WriteProcessMemory(hRemoteProcess,

pszLibFileRemote, (void \*)DllFullPath, lstrlen(DllFullPath) + 1, NULL) == 0)

{

MessageBox(NULL, L"将DLL的路径名复制到远程进程的内存空间失败", L"Error", MB\_OK);

return FALSE;

}