

IE浏览器UAF漏洞分析实战

by: bird

1. 分析环境

操作机: windows xp

windbg: 打开或附加 InternetExplore.exe 进程进行动态调试

IDA Pro: 打开 windows/system32/mshtml.dll 动态链接库, 加载完毕后用于行静态分析

2. 分析目的

熟悉释放后重用的调试方法, 熟悉浏览器漏洞的调试方法, !heap 命令的跟踪原理

通过逆向分析IE加载插件的过程, 学习释放后重用漏洞

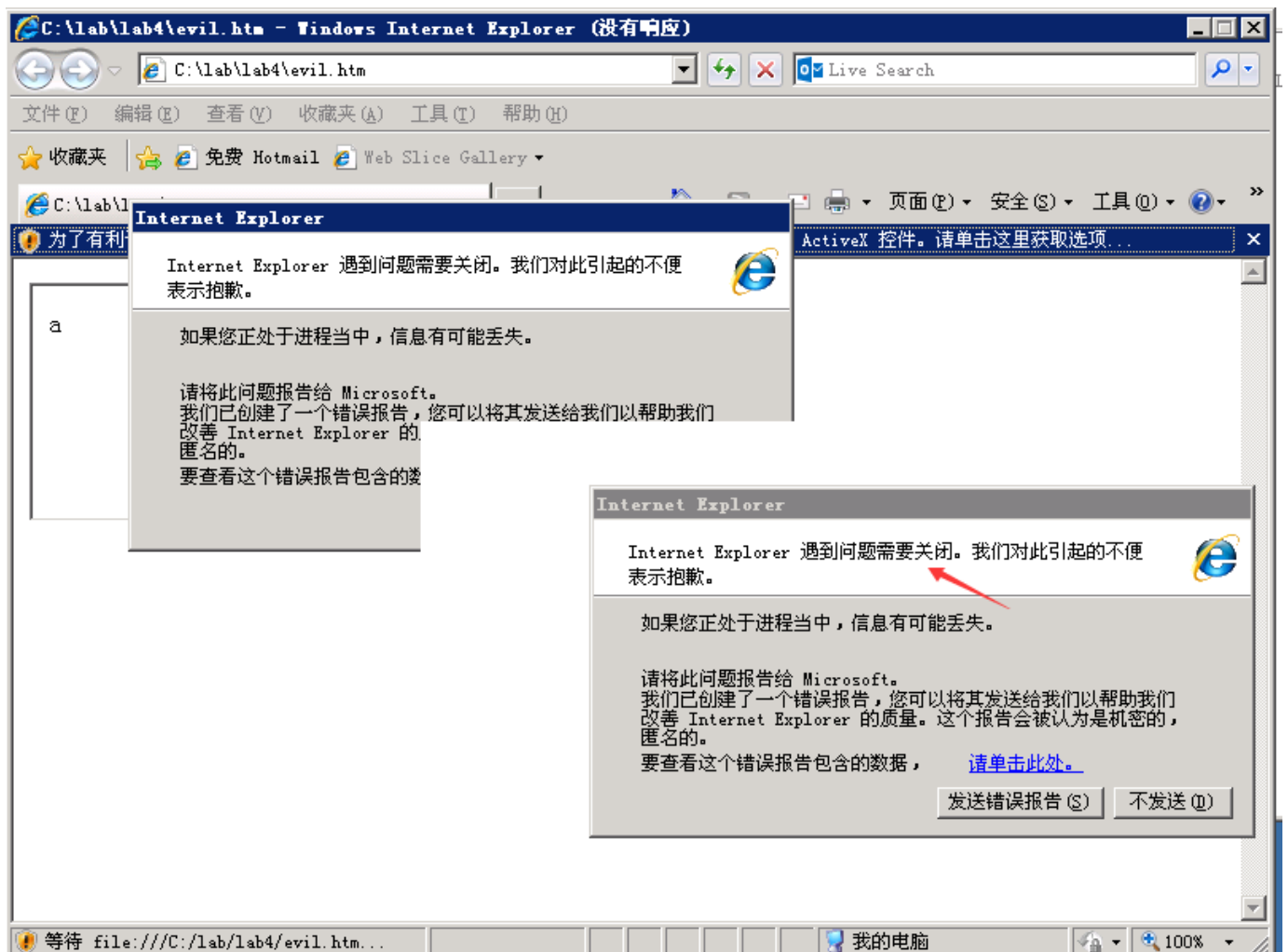
3. 漏洞原理

简单讲就是第一次申请的内存空间在释放过后没有进行内存回收, 导致下次申请内存的时候再次使用该内存块, 使得以前的内存指针可以访问修改过的内存

4. 分析步骤

步骤一: 打开 IE 浏览器

使用IE 浏览器打开evil.htm



IE 浏览器发生崩溃

步骤二：通过 Windbg 附加 IE 进程, 打开 poc动态调试

使用windbg 来附加IE 浏览器

```
Disassembly
Offset: @$scopeip
7c9211f9 0f85d7ec0000 jne ntdll!RtlDeactivateActivationContextUnsafeFast+0x28 (7c92fed6)
7c9211ff f6461010 test byte ptr [esi+10h],10h
7c921203 0f84cdec0000 je ntdll!RtlDeactivateActivationContextUnsafeFast+0x28 (7c92fed6)
7c921209 5e pop esi
7c92120a c9 leave esi
7c92120b c20400 ret 4
ntdll!DbgBreakPoint:
7c92120e cc int 3
7c92120f c3 ret
7c921210 8bff mov edi,edi
ntdll!DbgUserBreakPoint:
7c921212 cc int 3
7c921213 c3 ret

Command
ModLoad: 76d30000 76d48000 C:\WINDOWS\system32\iphlpapi.dll
ModLoad: 72240000 72245000 C:\WINDOWS\system32\sensapi.dll
ModLoad: 719c0000 719fe000 C:\WINDOWS\system32\mswsock.dll
ModLoad: 60fd0000 61025000 C:\WINDOWS\system32\hnetcfg.dll
ModLoad: 71a00000 71a08000 C:\WINDOWS\System32\wshtcpip.dll
ModLoad: 74cf0000 74d81000 C:\WINDOWS\system32\MLANG.dll
ModLoad: 5adc0000 5adf7000 C:\WINDOWS\system32\UxTheme.dll
ModLoad: 73640000 7366e000 C:\WINDOWS\system32\msctfime.ime
ModLoad: 76ef0000 76f17000 C:\WINDOWS\system32\DNSAPI.dll
ModLoad: 75e00000 75eae000 C:\WINDOWS\system32\SXS.DLL
ModLoad: 71cc0000 71cdb000 C:\WINDOWS\system32\actxprxy.dll
ModLoad: 76f90000 76f96000 C:\WINDOWS\system32\rasadhlp.dll
ModLoad: 63580000 63b2c000 C:\WINDOWS\system32\mshtml.dll
ModLoad: 05950000 05979000 C:\WINDOWS\system32\msls31.dll
ModLoad: 06210000 0623f000 C:\WINDOWS\system32\iepeers.dll
ModLoad: 72f70000 72f96000 C:\WINDOWS\system32\WINSPOOL.DRV
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msimtf.dll
ModLoad: 63380000 63434000 C:\WINDOWS\system32\jscript.dll
ModLoad: 1b000000 1b00c000 C:\WINDOWS\system32\imgutil.dll
ModLoad: 1b060000 1b06e000 C:\WINDOWS\system32\pngfilt.dll
ModLoad: 762f0000 762f5000 C:\WINDOWS\system32\msimg32.dll
(584.1b8): Break instruction exception - code 80000003 (first chance)
eax=7ffd6000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=07a3ffcc ebp=07a3fff4 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc int 3
```

之后g 运行，在IE 浏览器"allow blocked content" 来触发漏洞

```
Offset: @$scopeip
637d4639 ff751c push dword ptr [ebp+1Ch]
637d463c 8bf0 mov esi,eax
637d463e ff7518 push dword ptr [ebp+18h]
637d4641 ff7514 push dword ptr [ebp+14h]
637d4644 e820000000 call mshtml!CCommand::Exec (637d4669)
637d4649 8bf0 mov esi,eax
637d464b 8b7f08 mov edi,dword ptr [edi+8] ds:0023:067eaf80=????????
637d464e 8b07 mov eax,dword ptr [edi]
637d4650 57 push edi
637d4651 ff5008 call dword ptr [eax+8]
637d4654 8bc6 mov eax,esi
637d4656 5f pop edi
637d4657 5e pop esi

Command
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msimtf.dll
ModLoad: 76d70000 76d92000 C:\WINDOWS\system32\apphelp.dll
(168.334): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0687ffcc ebp=0687fff4 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc int 3
0:017> g
ModLoad: 63380000 63434000 C:\WINDOWS\system32\jscript.dll
(168.340): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000001f ecx=0657ef30 edx=0000000d esi=00000000 edi=067eaf78
eip=637d464b esp=038f8e80 ebp=038f8e8c iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
mshtml!CMshtmlEd::Exec+0x131:
637d464b 8b7f08 mov edi,dword ptr [edi+8] ds:0023:067eaf80=????????
0:008> dd edi
067eaf78 ???????? ???????? ???????? ????????
067eaf88 ???????? ???????? ???????? ????????
067eaf98 ???????? ???????? ???????? ????????
067eafa8 ???????? ???????? ???????? ????????
067eafb8 ???????? ???????? ???????? ????????
067eafc8 ???????? ???????? ???????? ????????
067eafd8 ???????? ???????? ???????? ????????
067eafe8 ???????? ???????? ???????? ????????
```

异常是由于edi+8指向了一个无效地址导致的

Disassembly

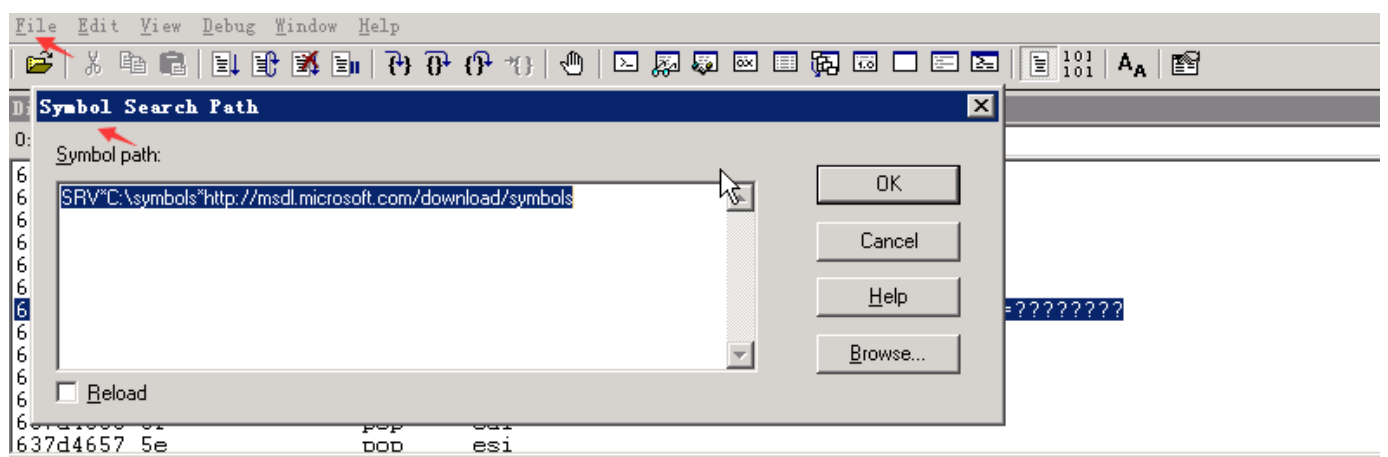
Offset: @\$scopeip

| | | | |
|----------|------------|------|---|
| 637d4639 | ff751c | push | dword ptr [ebp+1Ch] |
| 637d463c | 8bf0 | mov | esi,eax |
| 637d463e | ff7518 | push | dword ptr [ebp+18h] |
| 637d4641 | ff7514 | push | dword ptr [ebp+14h] |
| 637d4644 | e820000000 | call | mshtml!CCommand::Exec (637d4669) |
| 637d4649 | 8bf0 | mov | esi,eax |
| 637d464b | 8b7f08 | mov | edi,dword ptr [edi+8] ds:0023:066e2f80=???????? |
| 637d464e | 8b07 | mov | eax,dword ptr [edi] |
| 637d4650 | 57 | push | edi |
| 637d4651 | ff5008 | call | dword ptr [eax+8] |
| 637d4654 | 8bc6 | mov | eax,esi |
| 637d4656 | 5f | pop | edi |
| 637d4657 | 5e | pop | esi |

Command

ModLoad: 57fc0000 57fc8000 C:\WINDOWS\system32\msgsm32.acm
ModLoad: 57f90000 57f94000 C:\WINDOWS\system32\tssoft32.acm
ModLoad: 73ae0000 73ae7000 C:\WINDOWS\system32\tsd32.dll
ModLoad: 57fd0000 57fed000 C:\WINDOWS\system32\msg723.acm
ModLoad: 58000000 5804d000 C:\WINDOWS\system32\msaud32.acm
ModLoad: 57fa0000 57fbe000 C:\WINDOWS\system32\sl_anet.acm
ModLoad: 57e60000 57e99000 C:\WINDOWS\system32\iac25_32.ax
ModLoad: 58050000 580da000 C:\WINDOWS\system32\l3codeca.acm
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msintf.dll
ModLoad: 76d70000 76d92000 C:\WINDOWS\system32\appHelp.dll
ModLoad: 71cc0000 71cdb000 C:\WINDOWS\system32\actxprxy.dll
(330,620): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0699ffcc ebp=0699ff4 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc int 3
0:017> g
ModLoad: 63380000 63434000 C:\WINDOWS\system32\jscript.dll
(330,684): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=066eef30 edx=0000000d esi=00000000 edi=066e2f78
eip=637d464b esp=038f8e80 ebp=038f8e8c iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
mshtml!CCommand::Exec+0x131:
637d464b 8b7f08 mov edi,dword ptr [edi+8] ds:0023:066e2f80=????????

使用file-symbol加载一下符号表，勾选.reload 来重新加载符号表



加载之后可以看到相关函数的真实名称

```

Disassembly
Offset: @$scopeip
Previous Next
637d4639 ff751c      push    dword ptr [ebp+1Ch]
637d463c 8bf0        mov     esi,eax
637d463e ff7518      push    dword ptr [ebp+18h]
637d4641 ff7514      push    dword ptr [ebp+14h]
637d4644 e820000000  call   mshtml!CCommand::Exec (637d4669)
637d4649 8bf0        mov     esi,eax
637d464b 8b7f08      mov     edi,dword ptr [edi+8] ds:0023:067eaf80=????????
637d464e 8b07        mov     eax,dword ptr [edi]
637d4650 57          push    edi
637d4651 ff5008      call   dword ptr [eax+8]
637d4654 8bc6        mov     eax,esi
637d4656 5f          pop     edi
637d4657 5e          pop     esi

Command
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0687ffcc ebp=0687fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc          int     3
0:017> g
ModLoad: 63380000 63434000  C:\WINDOWS\system32\jscript.dll
(168.340): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=0657ef30 edx=0000000d esi=00000000 edi=067eaf78
eip=637d464b esp=038fbe80 ebp=038fbe8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CMshtmlEd::Exec+0x131:
637d464b 8b7f08      mov     edi,dword ptr [edi+8] ds:0023:067eaf80=????????
0:008> dd edi
067eaf78  ???????? ???????? ???????? ????????
067eaf88  ???????? ???????? ???????? ????????
067eaf98  ???????? ???????? ???????? ????????
067eafa8  ???????? ???????? ???????? ????????
067eafb8  ???????? ???????? ???????? ????????
067eafc8  ???????? ???????? ???????? ????????
067eafd8  ???????? ???????? ???????? ????????
067eafe8  ???????? ???????? ???????? ????????
0:008> .reload
Reloading current modules
.....

```

这个异常触发于CMshtmlEd类的Exec函数中

```

eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0687ffcc ebp=0687fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc          int     3
0:017> g
ModLoad: 63380000 63434000  C:\WINDOWS\system32\jscript.dll
(168.340): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=0657ef30 edx=0000000d esi=00000000 edi=067eaf78
eip=637d464b esp=038fbe80 ebp=038fbe8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CMshtmlEd::Exec+0x131:
637d464b 8b7f08      mov     edi,dword ptr [edi+8] ds:0023:067eaf80=????????
0:008> dd edi
067eaf78  ???????? ???????? ???????? ????????
067eaf88  ???????? ???????? ???????? ????????
067eaf98  ???????? ???????? ???????? ????????
067eafa8  ???????? ???????? ???????? ????????
067eafb8  ???????? ???????? ???????? ????????
067eafc8  ???????? ???????? ???????? ????????
067eafd8  ???????? ???????? ???????? ????????
067eafe8  ???????? ???????? ???????? ????????
0:008> .reload
Reloading current modules
.....

```

可以看到该异常为于mshtml.dll 中，通过Imm 来找到mshtml.dll 符号文件的位置

```
Disassembly
Offset: @$scopeip
Previous Next

637d4639 ff751c push dword ptr [ebp+1Ch]
637d463c 8bf0 mov esi, eax
637d463e ff7518 push dword ptr [ebp+18h]
637d4641 ff7514 push dword ptr [ebp+14h]
637d4644 e820000000 call mshtml!CCommand::Exec (637d4669)
637d4649 8bf0 mov esi, eax
637d464b 8b7f08 mov edi, dword ptr [edi+8] ds:0023:066e2f80=????????
637d464e 8b07 mov eax, dword ptr [edi]
637d4650 57 push edi
637d4651 ff5008 call dword ptr [eax+8]
637d4654 8bc6 mov eax, esi
637d4656 5f pop edi
637d4657 5e pop esi

Command
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msimtf.dll
ModLoad: 76d70000 76d92000 C:\WINDOWS\system32\appHelp.dll
ModLoad: 71cc0000 71cdb000 C:\WINDOWS\system32\actxprxy.dll
(330.620): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0699ffcc ebp=0699fff4 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc int 3
0:017> g
ModLoad: 63380000 63434000 C:\WINDOWS\system32\jscript.dll
(330.684): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=066eef30 edx=0000000d esi=00000000 edi=066e2f78
eip=637d464b esp=038f8e80 ebp=038f8e8c iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
mshtml!CmshtmlEd::Exec0x131:
637d464b 8b7f08 mov edi, dword ptr [edi+8] ds:0023:066e2f80=????????
0:008> .reload
Reloading current modules
0:008> lmm
^ Non-empty string required in 'lmm'
0:008> lmm mshtml
start end module name
63580000 63b2c000 mshtml (pdb symbols) c:\symbols\mshtml.pdb\ED5A6B679BD640A090E0A92342B253D22\mshtml.pdb
```

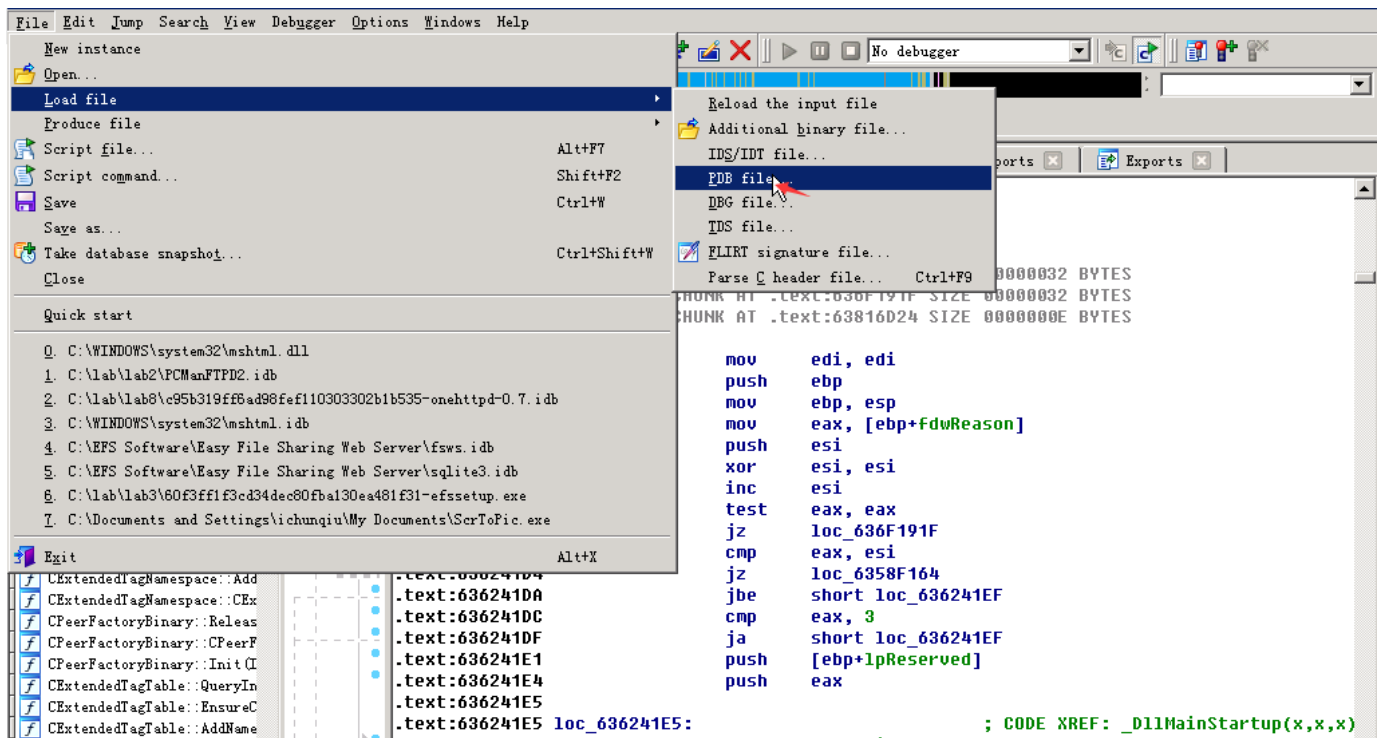
使用 lmm 来查看已经加载了的模块文件，可以看到 mshtml.dll 的位置

```
Disassembly
Offset: @$scopeip
Previous Next

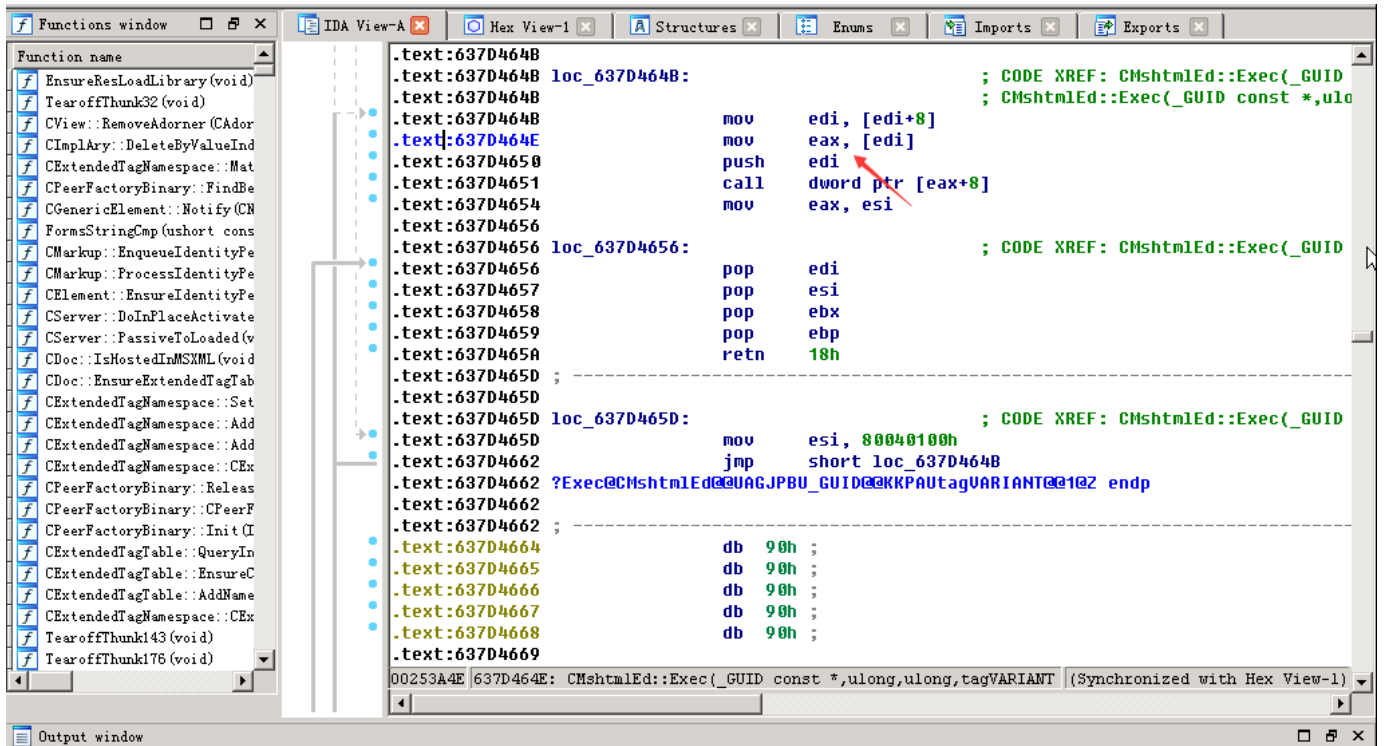
637d4639 ff751c push dword ptr [ebp+1Ch]
637d463c 8bf0 mov esi, eax
637d463e ff7518 push dword ptr [ebp+18h]
637d4641 ff7514 push dword ptr [ebp+14h]
637d4644 e820000000 call mshtml!CCommand::Exec (637d4669)
637d4649 8bf0 mov esi, eax
637d464b 8b7f08 mov edi, dword ptr [edi+8] ds:0023:066e2f80=????????
637d464e 8b07 mov eax, dword ptr [edi]
637d4650 57 push edi
637d4651 ff5008 call dword ptr [eax+8]
637d4654 8bc6 mov eax, esi
637d4656 5f pop edi
637d4657 5e pop esi

Command
58050000 580da000 l3codeca C:\WINDOWS\system32\l3codeca.acm
580e0000 580e7000 imaadp32 C:\WINDOWS\system32\imaadp32.acm
5ad00000 5adf7000 UxTheme C:\WINDOWS\system32\UxTheme.dll
5d170000 5d20a000 comctl32_5d170000 C:\WINDOWS\system32\comctl32.dll
5dba0000 5dba8000 rdpsnd C:\WINDOWS\system32\rdpsnd.dll
5dca0000 5de88000 iertutil C:\WINDOWS\system32\iertutil.dll
5fdd0000 5fe25000 NETAPI32 C:\WINDOWS\system32\NETAPI32.dll
62c20000 62c29000 LPK C:\WINDOWS\system32\LPK.DLL
63000000 630e6000 WININET C:\WINDOWS\system32\WININET.dll
63380000 63434000 jscript C:\WINDOWS\system32\jscript.dll
63580000 63b2c000 mshtml C:\WINDOWS\system32\mshtml.dll
71a10000 71a18000 WS2HELP C:\WINDOWS\system32\WS2HELP.dll
71a20000 71a37000 ws2_32 C:\WINDOWS\system32\ws2_32.dll
71cc0000 71cdb000 actxprxy C:\WINDOWS\system32\actxprxy.dll
72c60000 72c67000 msadp32 C:\WINDOWS\system32\msadp32.acm
72c80000 72c88000 msacm32 C:\WINDOWS\system32\msacm32.drv
73640000 7366e000 msctfime C:\WINDOWS\system32\msctfime.ime
73ae0000 73ae7000 tsd32 C:\WINDOWS\system32\tsd32.dll
73fa0000 7400b000 USP10 C:\WINDOWS\system32\USP10.dll
74650000 7467a000 msimtf C:\WINDOWS\system32\msimtf.dll
74680000 746cc000 MSCTF C:\WINDOWS\system32\MSCTF.dll
74cf0000 74d81000 Mlang C:\WINDOWS\system32\Mlang.dll
759d0000 75a7f000 USERENV C:\WINDOWS\system32\USERENV.dll
75e00000 75eae000 SXS C:\WINDOWS\system32\SXS.DLL
76060000 761b6000 SETUPAPI C:\WINDOWS\system32\SETUPAPI.dll
762d0000 762e0000 WINSTA C:\WINDOWS\system32\WINSTA.dll
76300000 7631d000 IMM32 C:\WINDOWS\system32\IMM32.DLL
76320000 76367000 comdlg32 C:\WINDOWS\system32\comdlg32.dll
76990000 76acd000 ole32 C:\WINDOWS\system32\ole32.dll
```

使用 IDA Pro 来打开 mshtml.dll，IDA Pro 会自动查询 mshtml.dll 的符号文件 或者指定一个符号文件



使用Jump->"Jump to address", 输入637d464e 来转到目标位置



为了查找edi 是如何传入的, 所以向上去查找


```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\My Documents>cd C:\Program Files\Debugging Tools for Windows (x86)

C:\Program Files\Debugging Tools for Windows (x86)>gflags.exe /I iexplore.exe +hpa
Current Registry Settings for iexplore.exe executable are: 02000000
hpa - Enable page heap

C:\Program Files\Debugging Tools for Windows (x86)>>
```

因为已经加载了符号表，在mshtml处下断点，按g运行，在浏览器中触发漏洞

```
Offset: @$scopeip
637d45b4 c20400      ret     4
637d45b7 90          nop
637d45b8 90          nop
637d45b9 90          nop
637d45ba 90          nop
637d45bb 90          nop
mshtml!CMshtmlEd::Exec:
637d45bc 8bff      mov     edi,edi
637d45be 55        push    ebp
637d45bf 8bec      mov     ebp,esp
637d45c1 53        push    ebx
637d45c2 56        push    esi
637d45c3 57        push    edi

Command
eip=7c92120e esp=0687ffcc ebp=0687fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc          int     3
0:017> bp mshtml!CMshtmlEd::Exec
Bp expression 'mshtml!CMshtmlEd::Exec' could not be resolved, adding deferred bp
0:017> .reload
Reloading current modules
0:017> bp mshtml!CMshtmlEd::Exec
Bp expression 'mshtml!CMshtmlEd::Exec' could not be resolved, adding deferred bp
0:017> bp mshtml!CMshtmlEd::Exec
Bp expression 'mshtml!CMshtmlEd::Exec' could not be resolved, adding deferred bp
0:017> bp mshtml!CMshtmlEd::Exec
0:017> bl
0 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
1 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
2 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
3 e 637d45bc 0001 (0001) 0:**** mshtml!CMshtmlEd::Exec
0:017> g
ModLoad: 63380000 63434000  C:\WINDOWS\system32\jscript.dll
Breakpoint 3 hit
eax=06426f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0684cff0 edi=00000000
eip=637d45bc esp=038fbc90 ebp=038fbc90 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec:
637d45bc 8bff      mov     edi,edi
```

单步执行到ebp+8，这个地方就是之前给漏洞现场赋值的地点

```

Disassembly
Offset: @$scopeip
637d45bc 8bff mov edi,edi
637d45be 55 push ebp
637d45bf 8bec mov ebp,esp
637d45c1 53 push ebx
637d45c2 56 push esi
637d45c3 57 push edi
637d45c4 8b7d08 mov edi,dword ptr [ebp+8] ss:0023:038f94=06426f78
637d45c7 8b4708 mov eax,dword ptr [edi+8]
637d45ca 8b08 mov ecx,dword ptr [eax]
637d45cc 50 push eax
637d45cd be00010480 mov esi,80040100h
637d45d2 ff5104 call dword ptr [ecx+4]
637d45d5 837d1403 cmp dword ptr [ebp+14h],3

Command
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x3:
637d45bf 8bec mov ebp,esp
0:008> p
eax=06426f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0684cff0 edi=00000000
eip=637d45c1 esp=038f94ebc ebp=038f94ebc iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x5:
637d45c1 53 push ebx
0:008> p
eax=06426f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0684cff0 edi=00000000
eip=637d45c2 esp=038f94ebc ebp=038f94ebc iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x6:
637d45c2 56 push esi
0:008> p
eax=06426f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0684cff0 edi=00000000
eip=637d45c3 esp=038f94eb4 ebp=038f94ebc iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x7:
637d45c3 57 push edi
0:008> p
eax=06426f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0684cff0 edi=00000000
eip=637d45c4 esp=038f94eb8 ebp=038f94ebc iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x8:
637d45c4 8b7d08 mov edi,dword ptr [ebp+8] ss:0023:038f94=06426f78

```

然后单步步过，输入! heap -p -a edi 查看堆的申请流程，最顶层的值就是目前edi所对应的值

```

Disassembly
Offset: @$scopeip
637d45be 55 push ebp
637d45bf 8bec mov ebp,esp
637d45c1 53 push ebx
637d45c2 56 push esi
637d45c3 57 push edi
637d45c4 8b7d08 mov edi,dword ptr [ebp+8]
637d45c7 8b4708 mov eax,dword ptr [edi+8] ds:0023:06426f80=04dd0f20
637d45ca 8b08 mov ecx,dword ptr [eax]
637d45cc 50 push eax
637d45cd be00010480 mov esi,80040100h
637d45d2 ff5104 call dword ptr [ecx+4]
637d45d5 837d1403 cmp dword ptr [ebp+14h],3
637d45d9 7470 je mshtml!CMshtmlEd::Exec+0x131 (637d464b)

Command
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0xb:
637d45c7 8b4708 mov eax,dword ptr [edi+8] ds:0023:06426f80=04dd0f20
0:008> !heap -p -a edi
address 06426f78 found in
_DPH_HEAP_ROOT @ 141000
in busy allocation ( DPH_HEAP_BLOCK: UserAddr UserSize - VirtAddr VirtSize)
662e500: 6426f78 88 - 6426000 2000
mshtml!CMshtmlEd::vftable'
7c938f01 ntdll!RtlAllocateHeap+0x00000e64
6359dab5 mshtml!CHTMLEditor::AddCommandTarget+0x00000020
6385ac44 mshtml!CHTMLEditor::GetCommandTarget+0x00000094
637d41c5 mshtml!CHTMLEditorProxy::GetCommandTarget+0x0000001e
637d4091 mshtml!CEditRouter::SetInternalEditHandler+0x00000064
637d4355 mshtml!CEditRouter::ExecEditCommand+0x000000ac
637be2fc mshtml!CDoc::ExecHelper+0x00000c91
638afda7 mshtml!CDocument::Exec+0x00000024
638ee2a9 mshtml!CBase::execCommand+0x00000050
638b167b mshtml!CDocument::execCommand+0x00000093
638e7445 mshtml!Method_VARIANTBOOLp_BSTR_oDoVARIANTBOOL_o0cVARIANT+0x00000149
636430c9 mshtml!CBase::ContextInvokeEx+0x000005d1
63643595 mshtml!CBase::InvokeEx+0x00000025
63643832 mshtml!DispatchInvokeCollection+0x0000014b
635e1cdc mshtml!CDocument::InvokeEx+0x000000f1
63642f30 mshtml!CBase::VersionedInvokeEx+0x00000020

```

现在第一个值所对应的就是CMshtmlEd所对应的一个对象

```

Disassembly
Offset: @scopeip
Previous
637d45be 55      push    ebp
637d45bf 8bec    mov     ebp,esp
637d45c1 53      push    ebx
637d45c2 56      push    esi
637d45c3 57      push    edi
637d45c4 8b7d08  mov     edi,dword ptr [ebp+8]
637d45c7 8b4708  mov     eax,dword ptr [edi+8] ds:0023:06426f80=04dd0f20
637d45ca 8b08    mov     ecx,dword ptr [eax]
637d45cc 50      push    eax
637d45cd be00010480 mov     esi,80040100h
637d45d2 ff5104  call   dword ptr [ecx+4]
637d45d5 837d1403 cmp     dword ptr [ebp+14h],3
637d45d9 7470    je      mshtml!CMshtmlEd::Exec+0x131 (637d464b)

Command
0:008> dps edi
06426f78 63639ea4 mshtml!CMshtmlEd::`vftable'
06426f7c 00000002
06426f80 04dd0f20
06426f84 064a1fc0
06426f88 0653cfd8
06426f8c 00000000
06426f90 00000000
06426f94 00000000
06426f98 00000000
06426f9c 00000000
06426fa0 00000000
06426fa4 00000000
06426fa8 00000000
06426fac 00000000
06426fb0 00000000
06426fb4 00000000
06426fb8 00000000
06426fbc 00000000
06426fc0 00000000
06426fc4 00000000
06426fc8 00000000
06426fcc 00000000

```

继续g运行，之前06426f80这里是有值的，可是现在里面的值没有了

也就是说cmshtml所对应的这个实例被释放了，但是后续Exec又会引用到这个edi，因此引用到了一个无效的地址，这个就是一个明显的释放后重用

```

637d4639 ff751c  push    dword ptr [ebp+1Ch]
637d463c 8bf0    mov     esi,eax
637d463e ff7518  push    dword ptr [ebp+18h]
637d4641 ff7514  push    dword ptr [ebp+14h]
637d4644 e820000000 call   mshtml!CCommand::Exec (637d4669)
637d4649 8bf0    mov     esi,eax
637d464b 8b7f08  mov     edi,dword ptr [edi+8] ds:0023:06426f80=????????
637d464e 8b07    mov     eax,dword ptr [edi]
637d4650 57      push    edi
637d4651 ff5008  call   dword ptr [eax+8]
637d4654 8bc6    mov     eax,esi
637d4656 5f      pop     edi
637d4657 5e      pop     esi

Command
06426fb0 00000000
06426fb4 00000000
06426fb8 00000000
06426fbc 00000000
06426fc0 00000000
06426fc4 00000000
06426fc8 00000000
06426fcc 00000000
06426fd0 00000000
06426fd4 00000000
06426fd8 00000000
06426fdc 00000000
06426fe0 00000000
06426fe4 00000000
06426fe8 00000000
06426fec 06426f78
06426ff0 00000000
06426ff4 00000000
0:008> g
(484.688): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000001f ecx=04dd0f30 edx=00000000 esi=00000000 edi=06426f78
eip=637d464b esp=038f8e80 ebp=038f8e8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CMshtmlEd::Exec+0x131:
637d464b 8b7f08  mov     edi,dword ptr [edi+8] ds:0023:06426f80=????????

```

打印所有和这个类有关的函数，发现调用了一个release函数，这个函数是针对cmshtml这个实例释放的过程

```

Disassembly
Offset: @$scopeip
Previous Next
637d4639 ff751c push dword ptr [ebp+1Ch]
637d463c 8bf0 mov esi,eax
637d463e ff7518 push dword ptr [ebp+18h]
637d4641 ff7514 push dword ptr [ebp+14h]
637d4644 e820000000 call mshtml!CCommand::Exec (637d4669)
637d4649 8bf0 mov esi,eax
637d464b 8b7f08 mov edi,dword ptr [edi+8] ds:0023:06426f80=????????
637d464e 8b07 mov eax,dword ptr [edi]
637d4650 57 push edi
637d4651 ff5008 call dword ptr [eax+8]
637d4654 8bc6 mov eax,esi
637d4656 5f pop edi
637d4657 5e ood esi

Command
06426fe0 00000000
06426fe4 00000000
06426fe8 00000000
06426fec 06426f78
06426ff0 00000000
06426ff4 00000000
0:008> g
(484.688): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=04dd0f30 edx=00000000 esi=00000000 edi=06426f78
eip=637d464b esp=038f8e80 ebp=038f8e8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
mshtml!CMshtmlEd::Exec+0x131:
637d464b 8b7f08 mov edi,dword ptr [edi+8] ds:0023:06426f80=????????
0:008> x mshtml!CMshtmlEd:*
637d3a90 mshtml!CMshtmlEd::Release = <no type information>
637d414d mshtml!CMshtmlEd::QueryInterface = <no type information>
6359daf2 mshtml!CMshtmlEd::Initialize = <no type information>
63639ef9 mshtml!CMshtmlEd::AddRef = <no type information>
63639ea4 mshtml!CMshtmlEd::vftable' = <no type information>
637d44f3 mshtml!CMshtmlEd::IsDialogCommand = <no type information>
637a82e7 mshtml!CMshtmlEd::QueryStatus = <no type information>
6374409c mshtml!CMshtmlEd::GetSegmentList = <no type information>
637d45bc mshtml!CMshtmlEd::Exec = <no type information>
6359de45 mshtml!CMshtmlEd::CMshtmlEd = <no type information>
6375bf32 mshtml!CMshtmlEd::~CMshtmlEd = <no type information>

```

再次在Exec这个函数入口地址下一个断点，看一下CMshtmlEd这个实例从存在到释放，到重用的整个过程

重新附加调试IE浏览器，在Exec函数下断点

```

Offset: @$scopeip
Previous Next
7c9211f9 0f85d7ec0000 jne ntdll!RtlDeactivateActivationContextUnsafeFast+0x28 (7c92fed6)
7c9211ff f6461010 test byte ptr [esi+10h],10h
7c921203 0f84cdec0000 je ntdll!RtlDeactivateActivationContextUnsafeFast+0x28 (7c92fed6)
7c921209 5e pop esi
7c92120a c9 leave
7c92120b c20400 ret 4
ntdll!DbgBreakPoint:
7c92120e cc int 3
7c92120f c3 ret
7c921210 8bff mov edi,edi
ntdll!DbgUserBreakPoint:
7c921212 cc int 3
7c921213 c3 ret

Command
ModLoad: 71cc0000 71cdb000 C:\WINDOWS\system32\actxprxy.dll
ModLoad: 76b10000 76b3a000 C:\WINDOWS\system32\WINMM.dll
ModLoad: 5dba0000 5dba8000 C:\WINDOWS\system32\rdpsnd.dll
ModLoad: 762d0000 762e0000 C:\WINDOWS\system32\WINSTA.dll
ModLoad: 5fdd0000 5fe25000 C:\WINDOWS\system32\NETAPI32.dll
ModLoad: 72c80000 72c88000 C:\WINDOWS\system32\msacm32.drv
ModLoad: 77bb0000 77bc5000 C:\WINDOWS\system32\MSACM32.dll
ModLoad: 580e0000 580e7000 C:\WINDOWS\system32\imaadp32.acm
ModLoad: 72c60000 72c67000 C:\WINDOWS\system32\msadp32.acm
ModLoad: 57ff0000 57ff5000 C:\WINDOWS\system32\msg711.acm
ModLoad: 57fc0000 57fc8000 C:\WINDOWS\system32\msgsm32.acm
ModLoad: 57f90000 57f94000 C:\WINDOWS\system32\tssoft32.acm
ModLoad: 73ae0000 73ae7000 C:\WINDOWS\system32\tsd32.dll
ModLoad: 57fd0000 57fed000 C:\WINDOWS\system32\msg723.acm
ModLoad: 58000000 5804d000 C:\WINDOWS\system32\msaud32.acm
ModLoad: 57fa0000 57fbe000 C:\WINDOWS\system32\sl_anet.acm
ModLoad: 57e60000 57e99000 C:\WINDOWS\system32\iac25_32.ax
ModLoad: 58050000 580da000 C:\WINDOWS\system32\l3codeca.acm
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msintf.dll
ModLoad: 76d70000 76d92000 C:\WINDOWS\system32\appHelp.dll
(150.510): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0675ffcc ebp=0675fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc int 3
0:017> bp mshtml!CMshtmlEd::Exec

```

按g运行，然后加载控件，加载之后命中了目标

```
Offset: @$scopeip
637d45b4 c20400      ret      4
637d45b7 90          nop
637d45b8 90          nop
637d45b9 90          nop
637d45ba 90          nop
637d45bb 90          nop
mshtml!CMshtmlEd::Exec:
637d45bc 8bff        mov     edi,edi
637d45be 55          push    ebp
637d45bf 8bec        mov     ebp,esp
637d45c1 53          push    ebx
637d45c2 56          push    esi
637d45c3 57          push    edi
Command
ModLoad: 72c60000 72c67000 C:\WINDOWS\system32\msadp32.acm
ModLoad: 57ff0000 57ff5000 C:\WINDOWS\system32\msg711.acm
ModLoad: 57fc0000 57fc8000 C:\WINDOWS\system32\msgsm32.acm
ModLoad: 57f90000 57f94000 C:\WINDOWS\system32\tssoft32.acm
ModLoad: 73ae0000 73ae7000 C:\WINDOWS\system32\tsd32.dll
ModLoad: 57fd0000 57fed000 C:\WINDOWS\system32\msg723.acm
ModLoad: 58000000 5804d000 C:\WINDOWS\system32\msaud32.acm
ModLoad: 57fa0000 57fbe000 C:\WINDOWS\system32\sl_anet.acm
ModLoad: 57e60000 57e99000 C:\WINDOWS\system32\iac25_32.ax
ModLoad: 58050000 580da000 C:\WINDOWS\system32\l3codeca.acm
ModLoad: 74650000 7467a000 C:\WINDOWS\system32\msimtf.dll
ModLoad: 76d70000 76d92000 C:\WINDOWS\system32\appHelp.dll
(150.510): Break instruction exception - code 80000003 (first chance)
eax=7ffd8000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c92120e esp=0675ffcc ebp=0675fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:
7c92120e cc          int     3
0:017> bp mshtml!CMshtmlEd::Exec
0:017> g
ModLoad: 63380000 63434000 C:\WINDOWS\system32\jscript.dll
Breakpoint 3 hit
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45bc esp=038fbc90 ebp=038fbc90 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec:
637d45bc 8bff        mov     edi,edi
```

继续F10单步跟踪到CMshtml赋值的地方

```
Offset: @$scopeip
637d45bc 8bff        mov     edi,edi
637d45be 55          push    ebp
637d45bf 8bec        mov     ebp,esp
637d45c1 53          push    ebx
637d45c2 56          push    esi
637d45c3 57          push    edi
637d45c4 8b7d08      mov     edi,dword ptr [ebp+8] ss:0023:038fbc94=06922f78
637d45c7 8b4708      mov     eax,dword ptr [edi+8]
637d45ca 8b08        mov     ecx,dword ptr [eax]
637d45cc 50          push    eax
637d45cd be00010480  mov     esi,80040100h
637d45d2 ff5104      call    dword ptr [ecx+4]
637d45d5 837d1403    cmp     dword ptr [ebp+14h],3
Command
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec+0x3:
637d45bf 8bec        mov     ebp,esp
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c1 esp=038fbc8c ebp=038fbc8c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec+0x5:
637d45c1 53          push    ebx
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c2 esp=038fbc84 ebp=038fbc8c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec+0x6:
637d45c2 56          push    esi
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c3 esp=038fbc80 ebp=038fbc8c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec+0x7:
637d45c3 57          push    edi
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c4 esp=038fbc78 ebp=038fbc8c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000202
mshtml!CMshtmlEd::Exec+0x8:
637d45c4 8b7d08      mov     edi,dword ptr [ebp+8] ss:0023:038fbc94=06922f78
```

步过之后edi的值是6922f78，因为是堆空间所以每次申请的值都不同

```

Disassembly
Offset: @$scopeip
637d45be 55      push    ebp
637d45bf 8bec    mov     ebp,esp
637d45c1 53      push    ebx
637d45c2 56      push    esi
637d45c3 57      push    edi
637d45c4 8b7d08  mov     edi,dword ptr [ebp+8]
637d45c7 8b4708  mov     eax,dword ptr [edi+8] ds:0023:06922f80=0396cf20
637d45ca 8b08    mov     ecx,dword ptr [eax]
637d45cc 50      push    eax
637d45cd be00010480 mov     esi,80040100h
637d45d2 ff5104  call    dword ptr [ecx+4]
637d45d5 837d1403 cmp     dword ptr [ebp+14h],3
637d45d9 7470    je      mshtml!CMshtmlEd::Exec+0x131 (637d464b)

Command
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0x5:
637d45c1 53      push    ebx
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c2 esp=038fbe88 ebp=038fbe8c iopl=0         nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000     efl=00000202
mshtml!CMshtmlEd::Exec+0x6:
637d45c2 56      push    esi
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c3 esp=038fbe84 ebp=038fbe8c iopl=0         nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000     efl=00000202
mshtml!CMshtmlEd::Exec+0x7:
637d45c3 57      push    edi
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=00000000
eip=637d45c4 esp=038fbe80 ebp=038fbe8c iopl=0         nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000     efl=00000202
mshtml!CMshtmlEd::Exec+0x8:
637d45c4 8b7d08  mov     edi,dword ptr [ebp+8] ss:0023:038fbe94=06922f78
0:008> p
eax=06922f78 ebx=6361bad0 ecx=63639ea4 edx=00000000 esi=0658eff0 edi=06922f78
eip=637d45c7 esp=038fbe80 ebp=038fbe8c iopl=0         nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000     efl=00000202
mshtml!CMshtmlEd::Exec+0xb:
637d45c7 8b4708  mov     eax,dword ptr [edi+8] ds:0023:06922f80=0396cf20

```

确认一下这个是不是cmshtml的一个实例，可以看到现在确实是属于CMshtml的一个实例

```

Offset: @$scopeip
637d45be 55      push    ebp
637d45bf 8bec    mov     ebp,esp
637d45c1 53      push    ebx
637d45c2 56      push    esi
637d45c3 57      push    edi
637d45c4 8b7d08  mov     edi,dword ptr [ebp+8]
637d45c7 8b4708  mov     eax,dword ptr [edi+8] ds:0023:06922f80=0396cf20
637d45ca 8b08    mov     ecx,dword ptr [eax]
637d45cc 50      push    eax
637d45cd be00010480 mov     esi,80040100h
637d45d2 ff5104  call    dword ptr [ecx+4]
637d45d5 837d1403 cmp     dword ptr [ebp+14h],3
637d45d9 7470    je      mshtml!CMshtmlEd::Exec+0x131 (637d464b)

Command
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::Exec+0xb:
637d45c7 8b4708  mov     eax,dword ptr [edi+8] ds:0023:06922f80=0396cf20
0:008> !heap -p -a edi
address 06922f78 found in
_DPH_HEAP_ROOT @ 141000
in busy allocation ( DPH_HEAP_BLOCK:      UserAddr      UserSize -      VirtAddr      VirtSize)
mshtml!CMshtmlEd::vftable'
7c938f01 ntdll!RtlAllocateHeap+0x00000e64
6359dab5 mshtml!CHTMLEditor::AddCommandTarget+0x00000020
6385ac44 mshtml!CHTMLEditor::GetCommandTarget+0x00000094
637d41c5 mshtml!CHTMLEditorProxy::GetCommandTarget+0x0000001e
637d4091 mshtml!CEditRouter::SetInternalEditHandler+0x00000064
637d4355 mshtml!CEditRouter::ExecEditCommand+0x000000ac
637be2fc mshtml!CDoc::ExecHelper+0x000003c91
638afda7 mshtml!CDocument::Exec+0x00000024
638ee2a9 mshtml!CBase::execCommand+0x00000050
638b167b mshtml!CDocument::execCommand+0x00000093
638e7445 mshtml!Method_VARIANTBOOLp_BSTR_oDoVARIANTBOOL_o0oVARIANT+0x00000149
636430c9 mshtml!CBase::ContextInvokeEx+0x0000005d1
63643595 mshtml!CBase::InvokeEx+0x00000025
63643832 mshtml!DispatchInvokeCollection+0x0000014b
635e1cdc mshtml!CDocument::InvokeEx+0x000000f1
63642f30 mshtml!CBase::VersionedInvokeEx+0x00000020

```

在刚才分析到的release函数在下一个断点


```
Offset: @$scopeip
637d45be 55      push    ebp
637d45bf 8bec    mov     ebp, esp
637d45c1 53      push    ebx
637d45c2 56      push    esi
637d45c3 57      push    edi
637d45c4 8b7d08  mov     edi, dword ptr [ebp+8]
637d45c7 8b4708  mov     eax, dword ptr [edi+8] ds:0023:06922f80=0396cf20
637d45ca 8b08    mov     ecx, dword ptr [eax]
637d45cc 50      push    eax
637d45cd be00010480 mov     esi, 80040100h
637d45d2 ff5104  call   dword ptr [ecx+4]
637d45d5 837d1403 cmp     dword ptr [ebp+14h], 3
637d45d9 7470    je      mshtml!CMshtmlEd::Exec+0x131 (637d464b)

Command
662fe28: 6922f78 88 - 6922000 2000
mshtml!CMshtmlEd::vitable'
7c938f01 ntdll!RtlAllocateHeap+0x00000e64
6359dab5 mshtml!CHTMLEditor::AddCommandTarget+0x00000020
6385ac44 mshtml!CHTMLEditor::GetCommandTarget+0x00000094
637d41c5 mshtml!CHTMLEditorProxy::GetCommandTarget+0x0000001e
637d4091 mshtml!CEditRouter::SetInternalEditHandler+0x00000064
637d4355 mshtml!CEditRouter::ExecEditCommand+0x000000ac
637be2fc mshtml!CDoc::ExecHelper+0x000003c91
638afda7 mshtml!CDocument::Exec+0x00000024
638ee2a9 mshtml!CBase::execCommand+0x00000050
638b167b mshtml!CDocument::execCommand+0x00000093
638e7445 mshtml!Method_VARIANTBOOLp_BSTR_oDoVARIANTBOOL_o0cVARIANT+0x00000149
636430c9 mshtml!CBase::ContextInvokeEx+0x0000005d1
63643595 mshtml!CBase::InvokeEx+0x00000025
63643832 mshtml!DispatchInvokeCollection+0x0000014b
635e1cdc mshtml!CDocument::InvokeEx+0x000000f1
63642f30 mshtml!CBase::VersionedInvokeEx+0x00000020

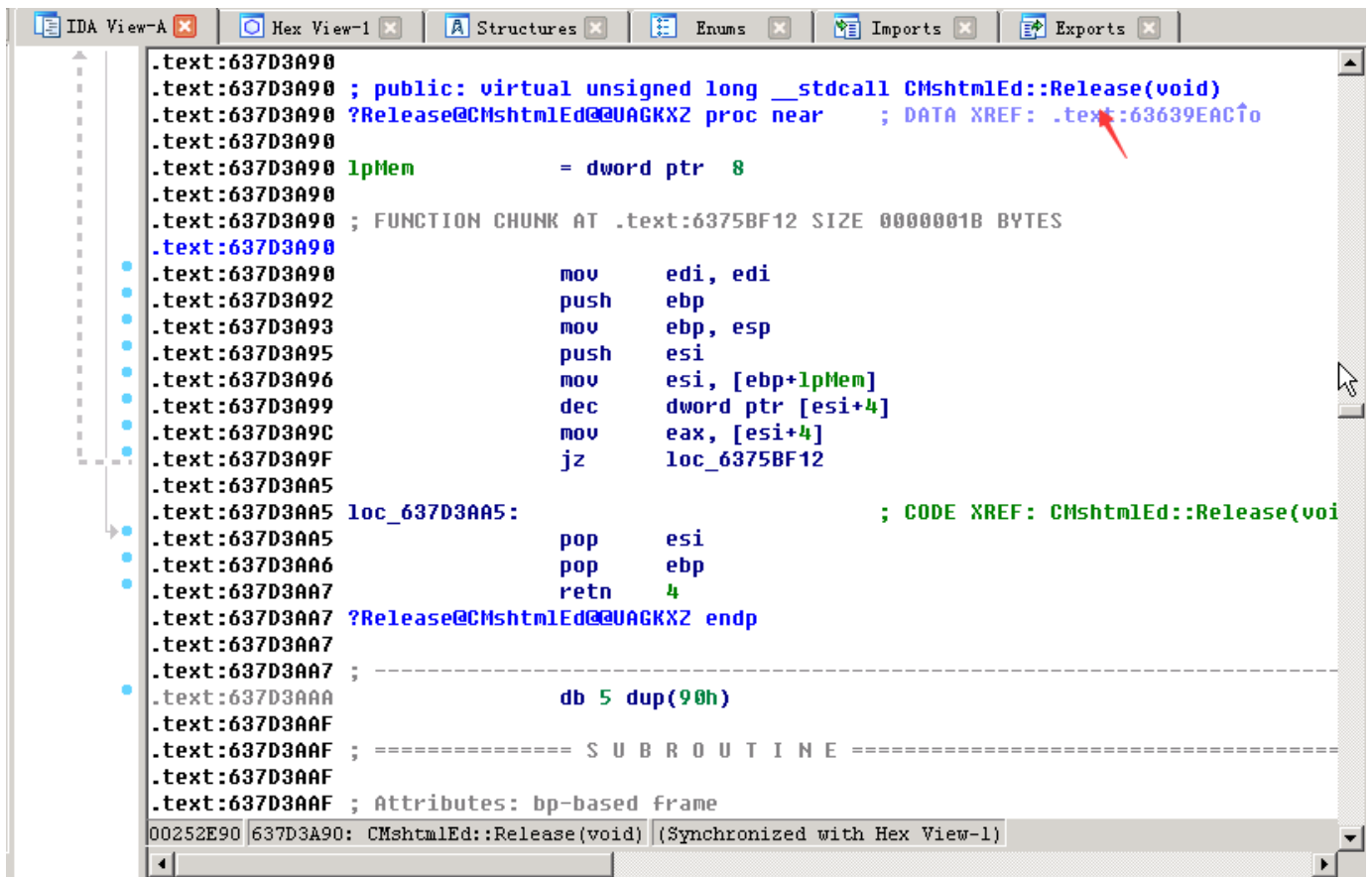
0:008> bp mshtml!CMshtmlEd::Release
0:008> bl
0 eu 0001 (0001) (mshtml!CMshtmlEd::Exec)
1 eu 0001 (0001) (mshtml!CMshtmlEd::Exec)
2 eu 0001 (0001) (mshtml!CMshtmlEd::Exec)
3 e 637d45bc 0001 (0001) 0:**** mshtml!CMshtmlEd::Exec
4 e 637d3a90 0001 (0001) 0:**** mshtml!CMshtmlEd::Release
```

在IDA里看一下这个函数

```
Functions window
Function name
f XHDC::GetClipBox(tagRECT *
f CImgCtx::TileFast CHDC con
f XHDC::BitBlt(int, int, int, i
f CTreeNode::GetParentWidth(
f IsTableCellNode(CTreeNode
f CFlowLayout::SizeCalcInfoF
f CRecalcLinePtr::Next(void)
f CLineCore::AO_GetFancyForm
f CFormElement::PrivateQuery
f CGeneratedContent::MarkupE
f CLayoutBlock::NonAnonymous
f CDisplayRequest::CDisplayR
f CDisplayRequest::SendForEl
f CDisplayRequest::Initializ
f CGeneratedContent::GetCont
f CDisplayRequest::Send(CMar
f CLayoutBlock::GetBlockCont
f TSmartPointer<CTableColumn
f CDisplayRequestGetClientOr
f CGeneratedContent::Doc(CTr
f CLinkElement::PrivateQuery
f TearoffThunk44(void)
f TearoffThunk81(void)
f CDisplayRequestGetRects::C
f CSpanElement::PrivateQuery
f CPhraseElement::PrivateQue
f CSelectionServices::GetMar
f CMshtmlEd::Release(void)
CMshtmlEd::release

IDA View-A
Hex View-1
Structures
Enums
Imports
Exports

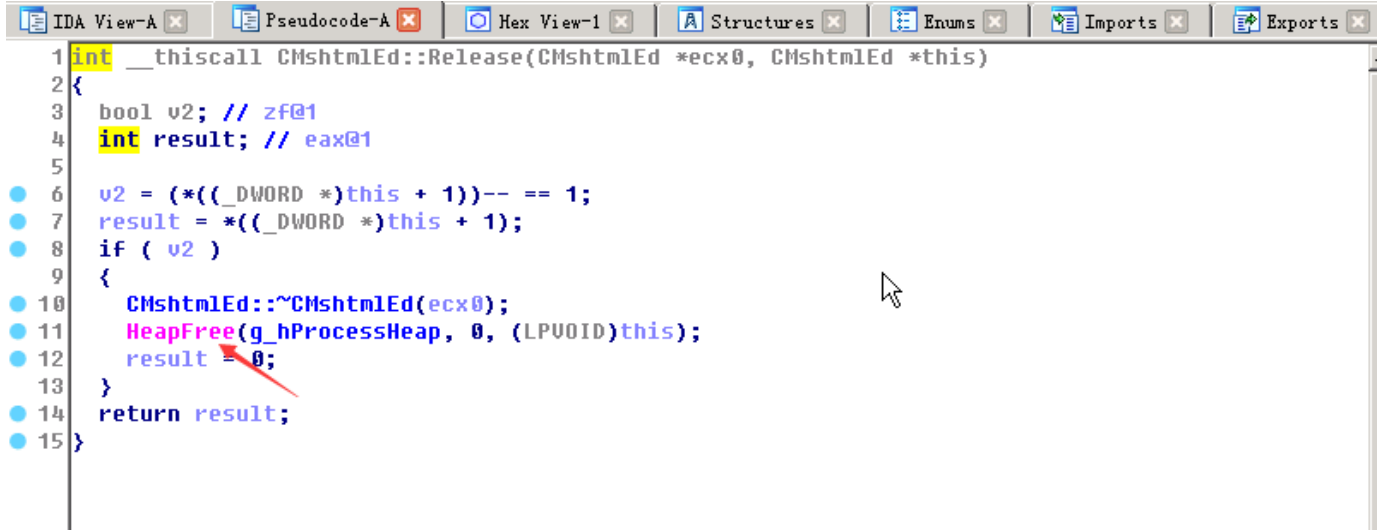
.text:637D4669 arg_0 = dword ptr 8
.text:637D4669 arg_4 = dword ptr 0Ch
.text:637D4669 arg_8 = dword ptr 10h
.text:637D4669 arg_C = dword ptr 14h
.text:637D4669
.text:637D4669 mov     edi, edi
.text:637D466B push    ebp
.text:637D466C mov     ebp, esp
.text:637D466E push    ecx
.text:637D466F push    edi
.text:637D4670 mov     eax, esi
.text:637D4672 call    ?GetLayout@CViewTask@@ABEPAUCLayout@@XZ ; CViewTask
.text:637D4677 xor     edx, edx
.text:637D4679 cmp     [ebp+arg_8], edx
.text:637D467C lea     ecx, [eax+10h]
.text:637D467F mov     eax, [ecx]
.text:637D4681 setz    dl
.text:637D4684 push    edx
.text:637D4685 call    dword ptr [eax+28h]
.text:637D4688 mov     [ebp+var_4], eax
.text:637D468B mov     eax, esi
.text:637D468D call    ?GetLayout@CViewTask@@ABEPAUCLayout@@XZ ; CViewTask
.text:637D4692 mov     edi, [ebp+arg_C]
.text:637D4695 call    ?PushCommandTarget@CHTMLEditor@@QAEJPAUCMshtmlEd@@@
.text:637D4698 mov     edi, eax
.text:637D469C test    edi, edi
.text:637D469E j1      short loc_637D46C8
.text:637D46A0 mov     eax, [esi]
.text:637D46A2 push    ebx
00253A7C 637D467C: CCommand::Exec(ulong,tagVARIANT *,tagVARIANT *,CMshta (Synchronized with Hex View-1)
```

The image shows the assembly view of the `CMshtmlEd::Release` function in IDA Pro. The assembly code is as follows:

```
.text:637D3A90
.text:637D3A90 ; public: virtual unsigned long __stdcall CMshtmlEd::Release(void)
.text:637D3A90 ?Release@CMshtmlEd@@UAGKXZ proc near ; DATA XREF: .text:63639EAC↑
.text:637D3A90 lpMem          = dword ptr 8
.text:637D3A90 ; FUNCTION CHUNK AT .text:63758F12 SIZE 0000001B BYTES
.text:637D3A90
.text:637D3A90      mov     edi, edi
.text:637D3A92      push    ebp
.text:637D3A93      mov     ebp, esp
.text:637D3A95      push    esi
.text:637D3A96      mov     esi, [ebp+lpMem]
.text:637D3A99      dec     dword ptr [esi+4]
.text:637D3A9C      mov     eax, [esi+4]
.text:637D3A9F      jz       loc_63758F12
.text:637D3AA5
.text:637D3AA5 loc_637D3AA5: ; CODE XREF: CMshtmlEd::Release(voi
.text:637D3AA5      pop     esi
.text:637D3AA6      pop     ebp
.text:637D3AA7      retn     4
.text:637D3AA7 ?Release@CMshtmlEd@@UAGKXZ endp
.text:637D3AA7 ; -----
.text:637D3AAA      db 5 dup(90h)
.text:637D3AAF
.text:637D3AAF ; ===== S U B R O U T I N E =====
.text:637D3AAF ; Attributes: bp-based frame
00252E90 637D3A90: CMshtmlEd::Release(void) (Synchronized with Hex View-1)
```

查看伪代码，发现确实执行了Heapfree这个操作，这个过程会把堆释放



The image shows the pseudocode view of the `CMshtmlEd::Release` function in IDA Pro. The pseudocode is as follows:

```
1 int __thiscall CMshtmlEd::Release(CMshtmlEd *ecx0, CMshtmlEd *this)
2 {
3     bool v2; // zf@1
4     int result; // eax@1
5
6     v2 = (*((__DWORD *)this + 1))-- == 1;
7     result = (*((__DWORD *)this + 1));
8     if ( v2 )
9     {
10         CMshtmlEd::~~CMshtmlEd(ecx0);
11         HeapFree(g_hProcessHeap, 0, (LPVOID)this);
12         result = 0;
13     }
14     return result;
15 }
```

继续跟踪一下这个释放的过程，g执行后断在了release函数

```

Offset: @$scopeip
637d3a88 c20800    ret     8
637d3a8b 90             nop
637d3a8c 90             nop
637d3a8d 90             nop
637d3a8e 90             nop
637d3a8f 90             nop
mshtml!CMshtmlEd::Release:
637d3a90 8bff          mov     edi,edi
637d3a92 55             push    ebp
637d3a93 8bec          mov     ebp,esp
637d3a95 56             push    esi
637d3a96 8b7508         mov     esi,dword ptr [ebp+8]
637d3a99 ff4e04         dec     dword ptr [esi+4]

Command
637d4355 mshtml!CEditRouter::ExecEditCommand+0x000000ac
637be2fc mshtml!CDoc::ExecHelper+0x000000c91
638afda7 mshtml!CDocument::Exec+0x000000024
638ee2a9 mshtml!CBase::execCommand+0x000000050
638b167b mshtml!CDocument::execCommand+0x000000093
638e7445 mshtml!Method_VARIANTBOOLp_BSTR_cDoVARIANT+0x000000149
636430c9 mshtml!CBase::ContextInvokeEx+0x0000005d1
63643595 mshtml!CBase::InvokeEx+0x000000025
63643832 mshtml!DispatchInvokeCollection+0x00000014b
635e1cdc mshtml!CDocument::InvokeEx+0x0000000f1
63642f30 mshtml!CBase::VersionedInvokeEx+0x000000020

0:008> bp mshtml!CMshtmlEd::Release
0:008> bl
0 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
1 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
2 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
3 e 637d45bc  0001 (0001) 0:**** mshtml!CMshtmlEd::Exec
4 e 637d3a90  0001 (0001) 0:**** mshtml!CMshtmlEd::Release
0:008> g
Breakpoint 4 hit
eax=06922f78 ebx=04b8a6a8 ecx=63639ea4 edx=00000012 esi=0658eff0 edi=00000000
eip=637d3a90 esp=038f8308 ebp=038f8370 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
mshtml!CMshtmlEd::Release:
637d3a90 8bff          mov     edi,edi

```

dps esi发现这个值是存在的

```

Offset: @$scopeip
637d3a88 c20800    ret     8
637d3a8b 90             nop
637d3a8c 90             nop
637d3a8d 90             nop
637d3a8e 90             nop
637d3a8f 90             nop
mshtml!CMshtmlEd::Release:
637d3a90 8bff          mov     edi,edi
637d3a92 55             push    ebp
637d3a93 8bec          mov     ebp,esp
637d3a95 56             push    esi
637d3a96 8b7508         mov     esi,dword ptr [ebp+8]
637d3a99 ff4e04         dec     dword ptr [esi+4]

Command
63643595 mshtml!CBase::InvokeEx+0x000000025
63643832 mshtml!DispatchInvokeCollection+0x00000014b
635e1cdc mshtml!CDocument::InvokeEx+0x0000000f1
63642f30 mshtml!CBase::VersionedInvokeEx+0x000000020

0:008> bp mshtml!CMshtmlEd::Release
0:008> bl
0 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
1 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
2 eu          0001 (0001) (mshtml!CMshtmlEd::Exec)
3 e 637d45bc  0001 (0001) 0:**** mshtml!CMshtmlEd::Exec
4 e 637d3a90  0001 (0001) 0:**** mshtml!CMshtmlEd::Release
0:008> g
Breakpoint 4 hit
eax=06922f78 ebx=04b8a6a8 ecx=63639ea4 edx=00000012 esi=0658eff0 edi=00000000
eip=637d3a90 esp=038f8308 ebp=038f8370 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
mshtml!CMshtmlEd::Release:
637d3a90 8bff          mov     edi,edi
0:008> dps esi
0658eff0  00000000
0658eff4  00000001
0658eff8  06922f78
0658effc  d0d0d0d0
0658f000  ????????
0658f004  ????????
0658f008  ????????
0658f00c  ????????

```

继续按g运行又断在release函数，单步过heapfree，esi已经被释放

```
Disassembly
Offset: @$scopeip
Previous Next

6375bf0d e915f9ffff jmp mshtml!CCommand::~CCommand (6375b827)
6375bf12 e81b000000 call mshtml!CMshtmlEd::~CMshtmlEd (6375bf32)
6375bf17 56 push esi
6375bf18 6a00 push 0
6375bf1a ff35a4d5aa63 push dword ptr [mshtml!g_hProcessHeap (63aad5a4)]
6375bf20 ff1568135863 call dword ptr [mshtml!_imp_HeapFree (63581368)]
6375bf26 33c0 xor eax, eax
6375bf28 e9787b0700 jmp mshtml!CMshtmlEd::~Release+0x27 (637d3aa5)
6375bf2d 90 nop
6375bf2e 90 nop
6375bf2f 90 nop
6375bf30 90 nop
6375bf31 90 nop

Command
0:008> p
eax=00000000 ebx=0396cf8c ecx=00000000 edx=0396cf8c esi=06922f78 edi=00000001
eip=6375bf1a esp=038f8278 ebp=038f8284 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
mshtml!CMshtmlEd::~Release+0x19:
6375bf1a ff35a4d5aa63 push dword ptr [mshtml!g_hProcessHeap (63aad5a4)] ds:0023:63aad5a4=00140000
0:008> p
eax=00000000 ebx=0396cf8c ecx=00000000 edx=0396cf8c esi=06922f78 edi=00000001
eip=6375bf20 esp=038f8274 ebp=038f8284 iopl=0 nv up ei pl zr na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
mshtml!CMshtmlEd::~Release+0x1f:
6375bf20 ff1568135863 call dword ptr [mshtml!_imp_HeapFree (63581368)] ds:0023:63581368={ntdll!RtlFreeHeap (7c92ff0d)}
0:008> p
eax=00000001 ebx=0396cf8c ecx=7c93003d edx=00145000 esi=06922f78 edi=00000001
eip=6375bf26 esp=038f8280 ebp=038f8284 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::~Release+0x25:
6375bf26 33c0 xor eax, eax
0:008> dd esi
06922f78 ???????? ???????? ???????? ????????
06922f88 ???????? ???????? ???????? ????????
06922f98 ???????? ???????? ???????? ????????
06922fa8 ???????? ???????? ???????? ????????
06922fb8 ???????? ???????? ???????? ????????
06922fc8 ???????? ???????? ???????? ????????
06922fd8 ???????? ???????? ???????? ????????
06922fe8 ???????? ???????? ???????? ????????
```

按g之后到了edi处于无效地址的位置

```
Offset: @$scopeip
Previous Next

637d463c 8bf0 mov esi, eax
637d463e ff7518 push dword ptr [ebp+18h]
637d4641 ff7514 push dword ptr [ebp+14h]
637d4644 e820000000 call mshtml!CCommand::Exec (637d4669)
637d4649 8bf0 mov esi, eax
637d464b 8b7f08 mov edi, dword ptr [edi+8]
637d464e 8b07 mov eax, dword ptr [edi] ds:0023:0c0c0c08=????????
637d4650 57 push edi
637d4651 ff5008 call dword ptr [eax+8]
637d4654 8bc6 mov eax, esi
637d4656 5f pop edi
637d4657 5e pop esi
637d4658 5b pop ebx

Command
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000246
mshtml!CMshtmlEd::~Release+0x1f:
6375bf20 ff1568135863 call dword ptr [mshtml!_imp_HeapFree (63581368)] ds:0023:63581368={ntdll!RtlFreeHeap (7c92ff0d)}
0:008> p
eax=00000001 ebx=0396cf8c ecx=7c93003d edx=00145000 esi=06922f78 edi=00000001
eip=6375bf26 esp=038f8280 ebp=038f8284 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00000202
mshtml!CMshtmlEd::~Release+0x25:
6375bf26 33c0 xor eax, eax
0:008> dd esi
06922f78 ???????? ???????? ???????? ????????
06922f88 ???????? ???????? ???????? ????????
06922f98 ???????? ???????? ???????? ????????
06922fa8 ???????? ???????? ???????? ????????
06922fb8 ???????? ???????? ???????? ????????
06922fc8 ???????? ???????? ???????? ????????
06922fd8 ???????? ???????? ???????? ????????
06922fe8 ???????? ???????? ???????? ????????
```

(150.24c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=0000001f ecx=0396cf30 edx=0000000d esi=00000000 edi=0c0c0c08
eip=637d464e esp=038f8280 ebp=038f828c iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206
mshtml!CCommand::Exec+0x134:
637d464e 8b07 mov eax, dword ptr [edi] ds:0023:0c0c0c08=????????

就是说此时esi被释放了，但是释放以后没有对this指针是否存在做一个标记和计数

看一下调用记录，freeheap释放了堆

```

Disassembly
Offset: eip
637d4639 ff751c      push    dword ptr [ebp+1Ch]
637d463c 8bf0        mov     esi, eax
637d463e ff7518      push    dword ptr [ebp+18h]
637d4641 ff7514      push    dword ptr [ebp+14h]
637d4644 e820000000  call    mshtml!CCommand::Exec (637d4669)
637d4649 8bf0        mov     esi, eax
637d464b 8b7f08      mov     edi, dword ptr [edi+8]
637d464e 8b07        mov     eax, dword ptr [edi]
637d4650 57          push    edi
637d4651 ff5008      call    dword ptr [eax+8]
637d4654 8bc6        mov     eax, esi

Command
0:008>
eax=00000000 ebx=0000001f ecx=05a74f30 edx=0000000d esi=05786fe8 edi=05d7ef78
eip=637d4649 esp=038f8e80 ebp=038f8e8c iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
mshtml!CmshtmlEd::Exec+0x128:
637d4649 8bf0        mov     esi, eax
0:008> !heap -p -a edi
address 05d7ef78 found in
_DPH_HEAP_ROOT @ 141000
in free-ed allocation ( DPH_HEAP_BLOCK:             VirtAddr             VirtSize)
                          5abd6d0:             5d7e000             2000
7c947553 ntdll!RtlFreeHeap+0x000000f9
769ad01c ole32!CRetailMalloc_Free+0x0000001c
769ad057 ole32!CoTaskMemFree+0x00000013
1a401f68 urlmon!operator delete+0x00000014
1a412285 urlmon!UriComponents::~UriComponents+0x00000022
1a40d5b0 urlmon!CreateUriPrivNoCache+0x0000005b
1a40d521 urlmon!CreateUriPriv+0x0000010d
1a403d60 urlmon!CreateUriWithFragment+0x0000001e
1a403d39 urlmon!CreateUri+0x00000018
63656596 mshtml!CDoc::NewDwnCtx+0x0000002e
63675345 mshtml!CIngHelper::FetchAndSetIngCtx+0x00000060
636752db mshtml!CIngHelper::SetIngSrc+0x00000023
63686e6d mshtml!CIngElement::OnPropertyChange+0x00000078
6366915a mshtml!BASICPROPPARAMS::SetStringProperty+0x0000021b
63680b58 mshtml!BASICPROPPARAMS::SetUriProperty+0x0000002f
6368a69f mshtml!CIngElement::put_src+0x0000001b

```

漏洞触发的原因是poc中申请的变量，有一个对src的初始化，然后会对src进行第二次赋值，在第二次赋值中从而引发了UAF漏洞

5. 总结

这是一个非常经典的UAF漏洞，此时当freeheap释放掉这个空间后，通过再次申请这个空间进行一个可控的占位，这样如果占位到了edi的值，那么后面的esi，eax都是可控的

```

637d45be 55          push    ebp
637d45bf 8bec        mov     ebp, esp
637d45c1 53          push    ebx
637d45c2 56          push    esi
637d45c3 57          push    edi
637d45c4 8b7d08      mov     edi, dword ptr [ebp+8]
637d45c7 8b4708      mov     eax, dword ptr [edi+8] ds:0023:06922f80=0396cf20
637d45ca 8b08        mov     ecx, dword ptr [eax]
637d45cc 50          push    eax
637d45cd be00010480  mov     esi, 80040100h
637d45d2 ff5104      call    dword ptr [ecx+4]
637d45d5 837d1403    cmp     dword ptr [ebp+14h].3
637d45d9 7470        je      mshtml!CmshtmlEd::Exec+0x131 (637d464b)

```

可以看到在三个地址后调用了有一个call函数，这个call是一个典型的虚函数调用，所以就可以通过这个call函数调用来进行一个跳转，将程序跳转到shellcode存放处，就可以达到代码执行的目的

