Windows 10 x64 edge 0day and exploit

exp-sky

Who am i ?

* Tencent’s Xuanwu Lab
* The security of browser
* Vulnerability discovery
* Exploit technique

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

Windows 10 x64 and edge

Widnows 10 x64

Windows 10 x64 and edge

减少攻击面：

vml,兼容性,旧引擎 …

增加保护机制：

CFG,MemGC,Win32k filter …

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

DEP

* Data Execution Prevention (DEP)
  * Windows XP SP2
  * Windows Server 2003 SP1

DEP

memory
buffer overflow
Function 1 buffer
Function 1 ret addr
Function 2 var
Function 2 ret addr
rip
= ret_addr
= shell code addr

DEP

DEP

* ROP

```
//mshtml + 0x002C1397 : ,# RETN 0x30
//mshtml + 0x004e3cc1 : ,# RETN
//mshtml + 0x004e3cbf : ,# PUSH ECX # POP ESP ; RET
//mshtml + 0x001178C0 : ,# POP EAX # RETN
//mshtml + 0x005D8888 : ,# MOV EAX,DWORD PTR DS:[EAX] # RETN
//mshtml + 0x007EFB12 : ,# XCHG EAX,ESI # RETN
//mshtml + 0x002E5291 : ,# POP EBP # RETN
//mshtml + 0x000B2269 : ,# & JMP ESP
//mshtml + 0x00883314 : ,# POP EAX # RETN
//mshtml + 0x0038F5F0 : ,# NEG EAX # RETN
//mshtml + 0x003DD7B9 : ,# XCHG EAX,EBX # RETN
//mshtml + 0x0039C4EF : ,# XCHG EAX, EBX # RETN 0x0014
//mshtml + 0x004e3cc1 : ,# RETN ;
//mshtml + 0x0088324C : ,# POP EAX # RETN
```

DEP

* VirtualProtect

```
int Memory::SmallHeapBlockT<SmallAllocationBlockAttributes>
::ClearPageHeapState(void *p_struct)
{
    DWORD old_protect = 0;
    QWORD ret;

    if ( p_struct->buffer )
    {
        ret = VirtualProtect(p_struct->buffer, 0x1000,
                             p_struct->new_protect, &old_protect);
    }
    return ret;
}
```

DEP

```
0:033> !address 0000015f`e5bbc020
Usage:                  <unknown>
Base Address:           0000015f`e5bb0000
End Address:            0000015f`e5bbf000
Region Size:            00000000`0000f000 (   60.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000004          PAGE_READWRITE
```

call VirtuaProtect

```
0:033> !address 0000015f`e5bbc020
Usage:                  <unknown>
Base Address:           0000015f`e5bb0000
End Address:            0000015f`e5bbf000
Region Size:            00000000`0000f000 (   60.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000040          PAGE_EXECUTE_READWRITE
```

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

ASLR

* Address space layout randomization (ASLR)
  * linux 2001-07
  * Windows Vista 2007-01

ASLR

ASLR

```
0:021> dq 000001cb`bb76c100
000001cb`bb76c100  00007ff9`92e21988 000001cb`a5720f80
000001cb`bb76c110  00000000`00000000 00000000`00000005
000001cb`bb76c120  00000000`0000002a 000001cb`bb76c140
000001cb`bb76c130  000001cb`bb76c140 000001cb`a36cb920
000001cb`bb76c140  0000002a`00000000 00000000`0000002a
000001cb`bb76c150  00000000`00000000 0c0c0c0c`0c0c0c0c
000001cb`bb76c160  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c170  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
```

```
000001cb`bb76c180  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c190  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1a0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1b0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1c0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1d0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1e0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
000001cb`bb76c1f0  0c0c0c0c`0c0c0c0c 0c0c0c0c`0c0c0c0c
```

ASLR

ASLR

127.0.0
此站点提示...
shell code address : 0x28e8830f020
不要让这个页面创建更多消息
确定

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

MemGC = Memory Protection + GC

MemGC

* Unprotected object.
* The object pointer is not on the stack when released.
* Double free.

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

CFG

* Control Flow Guard (CFG)

```
mov     eax, [edi]
call    dword ptr [eax+0A4h]
```

```
mov     eax, [edi]
mov     esi, [eax+0A4h] ; esi = virtual function
mov     ecx, esi
call    ds:___guard_check_icall_fptr //ntdll!LdrpValidateUserCallTarget
mov     ecx, edi
call    esi
```

CFG

bitmap
index offset : data
[0x0077b960] 0x01dee58c : 0x55555555
[0x0077b964] 0x01dee590 : 0x30010555
[0x0077b968] 0x01dee594 : 0x04541041
...
bt : 0x30010555&0x400 != 0
00000100 00000000 = 0x400
01010 = 0x0a = 10
function
address : 0x77b96450
0x77b96450 : [01110111 10111001 01100100 01010000]

CFG

```
int __cdecl Js::JavascriptFunction::DeferredParsingThunk(
    struct Js::ScriptFunction *p_script_function)
{
  function_point = Js::JavascriptFunction::DeferredParse(&p_script_function);
  return function_point();
}
```

```
.text:002AB3F0 push    ebp
.text:002AB3F1 mov     ebp, esp
.text:002AB3F3 lea     eax, [esp+p_script_function]
.text:002AB3F7 push    eax             ; struct Js::ScriptFunction **
.text:002AB3F8 call    Js::JavascriptFunction::DeferredParse
.text:002AB3FD pop     ebp
.text:002AB3FE jmp     eax
```

CFG

```
0:010> g
Breakpoint 0 hit
eax=603ba064 ebx=063fba10 ecx=063fba40 edx=063fba40 esi=00000001 edi=058fc6b0
eip=603ba064 esp=058fc414 ebp=058fc454 iopl=0         nv up ei ng nz na po cy
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000283
chakra!`dynamic initializer for 'DOMFastPathInfo::getterTable''+0x734:
603ba064 94              xchg    eax,esp
603ba065 c3              ret
```

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

Exploit

* Full Memory Read/Write

Exploit

* bypass ASLR
* bypass DEP
* bypass MemGC
* bypass CFG

Exploit

RuntimeBroker.exe		34,240 K	3128	Runtime Broker	Microsoft Corporation	64-bit	DEP (permanent)	Medium	ASLR
MicrosoftEdgeCP.exe		2,981,508 K	5948	Microsoft Edge Conten...	Microsoft Corporation	64-bit	DEP (permanent)	AppContainer	ASLR
cmd.exe		3,180 K	5472	Windows 命令处理程序	Microsoft Corporation	64-bit	DEP (permanent)	AppContainer	ASLR
conhost.exe	< 0.01	8,716 K	5344	Console Window Host	Microsoft Corporation	64-bit	DEP (permanent)	AppContainer	ASLR

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

Demo

```
0:009> r
rax=0000007784725798 rbx=0000007784725530 rcx=1111111111111111
rdx=000001b39fef82c0 rsi=0000000000000002 rdi=0000007784725040
rip=00007ffe7a34eae9 rsp=0000007784725770 rbp=00000000000003f1
 r8=000001bba4e7fd18  r9=000001b39fe943d0 r10=00007ffe7634ca90
r11=00000077847253e0 r12=000001bba19afde0 r13=00007ffe92fe77d0
r14=00007ffe92fe77d0 r15=000000007c190422
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010204

cmp     byte ptr [rcx],0 ds:11111111`11111111=??
```

```
or      dword ptr [rbx+60h], 0FFFFFFFFh    //memory write
```

此电脑
工具
cmd
index.html
child_1.html
Web_Serv...
127.0.0
此站点提示...
edit ok
确定
回收站
17:20
2016/7/14

Demo

```
0:010> r
rax=1111111111111111 rbx=0000008c4a8fcef0 rcx=00000258d9c30340
rdx=0000000000000000 rsi=0000000000000002 rdi=0000008c4a8fca00
rip=00007ffd1d2ce6b1 rsp=0000008c4a8fd130 rbp=0000000000000000
 r8=00000258d9ce5052  r9=00000258d9ce5052 r10=00000258d9ce5050
r11=0000008c4a8fd040 r12=0000000000000000 r13=00000000000000d2
r14=00000258d999dae0 r15=00000000000003ee
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010204

mov     rsi,qword ptr [rax] ds:11111111`11111111
```

```
mov     dword ptr [rsi+30h],1    //memory write
```

此电脑

工具

cmd

index.html

child_1.html

child_2.html

Web_Serv...

127.0.0

此站点提示...

edit size ok : 0xffffff2a

不要让这个页面创建更多消息

确定

127.0.0.1 想要使用你的位置，但首先，你需要转到"设置"并启用"定位"。

打开设置

回收站

16:06
2016/7/14

Windows 10 x64 edge 0day and exploit

* Windows 10 x64 and edge
* DEP
* ASLR
* MemGC
* CFG
* Exploit
* Demo
* Q&A

Q&A

weibo : exp-sky
twitter : exp-sky
blog : http://www.exp-sky.org/blog