【学习笔记】通过样本分析之二CVE-2010-3333

diffway / 2017-06-26 06:36:00 / 浏览数 9115 新手 入门资料 顶(0) 踩(0)

1 分析环境

- 操作系统：window xp sp3
- 软件　：office 2003

2 基本信息

- 漏洞类型：栈溢出
- 影响范围：Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011

3 样本分析

样本MD5：f5da6e333729a9809e3c0abaff619665

样本名称：過程論的觀點分析六方會談 審查意見.doc

首先在我们拿到样本在不知道CVE编号的情况下，还是先通过行为来查看一下，好进行下断点，我们可以看到这个样本在临时文件夹释放了一个PE文件，并将这个PE文件执行

我们先下一个执行程序的断点

我们可以看到第一个参数为执行的文件路径，而返回地址确实栈地址，我们返回到这个返回地址

我们在返回地址清楚的看到了执行的shellcode,这也表明这是个栈溢出

我们顺着shellcode往上看，看到了三个909090，比较明显的nop指令,我们接着反编译一下这个地址，发现这个是shellcode的开头，下面是比较明显的获取PEB的地址的代

我们开始向上看，可以找到几个返回地址，我们在这个返回地址下断点

我们成功断刀 mso 模块的 3107f609，这个时候我们开始定位栈溢出地址

发现是mso这个模块中的某个函数返回后执行了经典的jmp esp 来执行shellcode

这个时候我们将mso这个模块放到IDA中，来仔细的查看是什么地方出现了问题，动态调试发现是执行了这个函数返回的时候跳转到jmp esp
的，我们重点关注下这个函数

30F4cc5d

这个时候我们在返回地址下个内存写断点，同时关注下返回地址,可以定位到时那句代码导致的返回地址被覆盖

最终我们定位到了是下面的拷贝导致的返回地址被覆盖

而控制复制长度主要是ecx,我们看到ecx在文档的什么位置

通过分析发现，这个ecx正式样本下面框的位置，而样本的后面就是经典的跳转地址，和shellcode。

而我们看到栈地址开辟的地址只有14h个字节

这个时候再能控制复制大小的情况下和能控制shellcode的情况下，就能从容的写出利用。

我们这个时候看下利用，这个攻击样本并没有考虑到如ALSR和DEP的保护机制，而是直接通过一个XP下的经典跳转地址7ffa4512将EIP控制成为esp,来执行shellcode。She

总结

这个漏洞还是比较简单的栈溢出，利用也比较简单，正是因为这个比较好控制，所以也成为各个APT组织的重点使用对象，经常出现在各个攻击中。

上一篇：【讨论】大家平常都如何整理知识笔记... 下一篇：绕过AppLocker系列之MSI...

1. 0 条回复
   - 动动手指，沙发就是你的了！

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