【学习笔记】通过样本分析之三CVE-2011-0104

diffway / 2017-07-03 01:45:00 / 浏览数 3622 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 sp3

2 基本信息

漏洞类型：栈溢出

影响范围：Microsoft Excel 2002 SP3 and 2003 SP3, Office 2004 and 2008 for Mac

3 漏洞分析

Exp MD5: fbd4378af4ef2e249a6a81e1ba12db99

由于并没有找到对应的在实际攻击中的样本，这里我们使用Abysssec团队放出的exp

进行调试。

我们上windbg进行分析，我们的样本的并没有弹出那个计算器，我们现在打开Excel,

然后用windbg附加上，然后打开样本，有个异常错误。

我们首先将Excel.exe放到IDA中，然后查看这个地址属于哪个函数，在函数开头下断点，

在返回地址处，下个内存写断点，我们可以发现循环拷贝的地方导致覆盖了返回地址。

我们重点关注下这个地址。

首先我们先确定一下拷贝的函数在文件的位置

这是个循环复制，，第一次ECX为1，只复制了四个字节，我们用offVIS打开文件，发

现复制的是BOF字段的阴影中的四个字节。

我们看看第二次复制的情况，第二次复制的是从下面阴影开始的字段

而要复制的字段明显的超过栈空间，因为这个栈空间只有60h个字节，而复制的

而复制的要有300字节，导致栈溢出。

当我们知道了可以控制覆盖的数据的时候，还要去了解整个ECX是从何处来的，这个时

候我们断到溢出函数的起点来看看EXC来自的文件的何处。

我们在将上一层函数在IDA反汇编成伪代码，发现函数在执行之前会比较一下是否是A7。

在来看看Abysssec团队写的生成EXP的python脚本，我们发现了这个A7是recordTypt

我们再次打开OffVIS,我们可以看到这个是BIFFRecord

我们在往下看代码

我们发现sub_300DE7C5 返回的是3c跟比较的相同，

这个时候我们发现BIFFRecord下面的Contine 的Type也正是0x3c，经过我的实验，我

将这个3c改成其他的数，在动态调试，返现sub_300DE7C5这个函数返回的正式Continue的Type

我们继续调试，发现sub_300C3AA4返回的是Continue的长度，正式Continue的length字段，这个字段是的长度也是0x300,这个时候，我们可以肯定的就是这个Continue

在次看Continue 字段的最后一个值 ContinueDate，正是复制的字段。

其实这个能实现完美利用的关键还在于，这个漏洞可以控制复制到那个位置，我们来看一下

首先这个先从ebp+34h的地方取出0c0f,后来又乘以了4

通过实验我们发现这两个就是BIFFRecord的Length 和Data

这两个相乘后，作为偏移加上eax放到 esi中

最后esi作为参数放入拷贝函数中，而这个就是拷贝的目标地址，这样我们就可以实现目标地址定位。

总结

这个漏洞通过栈溢出可以通过控制拷贝大小，拷贝位置实现精确控制，开发者在拷贝的时候，并没有对拷贝的大小进行控制。

上一篇：【译】骚年，看我如何把Phanto... 下一篇：Thinkphp5X设计缺陷导致泄...

1. 1 条回复

c0de 2017-07-05 06:37:24

不错。

0 回复Ta
