IE GC信息泄漏这个漏洞的八卦

这个漏洞是早几个月dion牛放出的，最近还得了pwnie award的奖，原文中讲了flash，ff等的GC引擎都采用保守的标记清除算法并且都没有标记出数据还是指针，所以都存在这个问题，dion牛的来路相信大家都不陌生，不知道的搜搜flash jit spray，刚刚查了一下，这位神牛也去FireEye了，从时间上来看，好像他刚刚发完这个东西后就去了。他说他研究了一周多点搞定原理并写了flash和ff的poc。Flash有dictionary对象，并且支持遍历，可能不会花多久时间，ff稍有难度，但借助源码，dion牛也没给出一个可用的poc，但即便是这样，这种效率还是让人绝望和心碎。回头说yuange，yuange在09年就在ie9中发现这个漏洞了，用的方法是人肉数据流跟踪，t的时候读懂算法，（之前可能也读了chrome的标记清除算法？）这种功力想必是人人都想拥有却可遇不可求了。不得不说yuange不仅选矿眼光独到，人肉挖矿能力更是一流。这个漏洞Dion是看脚本引擎的源码看出来的，yuange是看反汇编加调试发现的，从时间上来说发现更早，pwnie award的奖也没有提yuange一下啊。

然后就是yuange和ms的漏洞定性之争了，大家热情都很高，一起参与进来，好不热闹。好像扯远了，说完了漏洞发现，来说说漏洞利用。能push可控数据让gc当成指针标记并在sweep时将本来应该删除的对象不删除，也就是说在js语法层面已经引用不到对象，但gc不会清除，很明显这是内存泄露，但如果有方法探测到这些对象是不是还存在于内存中，就能靠猜泄露出对象地址。找到方法能在脚本层面引用或者计数这些本应被删除但实际没被删除的对象，这是很正常的思路，dion在flash中发现了dictionary，弱引用关系，不增加对象引用计数，该删除时就删除，还能遍历探测内存中是否确实删除了，好像专门为此漏洞的利用量身定做的一样，基于遍历特性还能一次猜多个，真是太给力了。类似的在ff和ie11中有weakmap，但不支持遍历，想探测就困难了。Dion牛提出了timing attack，timer标识，能产生io效应的对象三个思路，最后集中在timing attack上，在ff上搞了一半放弃了。

其实timing attack在ie11上还是行的通的。算法不同但写代码的人的思路总是一致的。在ie11中用timing attack要解决几个问题，一是要保证时间结果不出错的问题，这个在了解weakmap的set方法的算法之后能准确的控制，能准确到什么程度，和flash的dictionary一样，能知道gc是否成功，能知道对象是否未删除，甚至能知道猜对了几个地址，原理dion已经说了，就是填满weakmap的hash表，看set方法是否会导致耗费时间的扩容hash表并进行拷贝的操作；另一个就是暴力猜的时间复杂度问题，用空间复杂度换时间复杂度是个不错的方法，思路就是减少随机猜测的熵，但随机猜还是顺序猜，用多少空间换多少时间，这还需要进一步考量和优化，这也是我说的时延和概率问题，如果猜好几分钟才猜到，那就真的成了一个名副其实的poc了；再一个就是push多个猜多个的问题，push多个固然好，概率大大增加，但不像dictionary可以遍历，push多个如果猜对还是不知道是哪个，如果push一个spray多个被猜对象，能一次猜多个，大大增加猜中的概率；最后一个就是猜什么的问题，这个很关键，影响着到底能不能猜出来的最终结果，选择合适的对象大小使得后几位地址对齐的对象（比如0x100/0xfc）是个选择，但不够好，用array中的数据成员的地址指针是个不错的方法（前提是你知道不光对象地址，对象中成员的地址也能骗过gc），因为你可控制array大小使得对齐地址变成后四位，也就是说除去高位的0和低四位，只用猜测3位，甚至由于猜多个产生的小spray效应使得只用猜测2位，那么效率将会大大提高。

其实利用中有timing和暴力猜测两个因素就已经决定利用代码肯定不会完美了，但本着为人民服务的原则还是坚持完成了version1。中间各种方法的选择尝试，研究这个比写个典型的一个堆溢出漏洞过全部保护机制的要蛋疼多了，堆布局，时间复杂度，gc，weakmap算法等等了。总的来说算是一个投入产出比不高的事情。

至于泄露出的地址能做神马，大家就可以尽情发挥想象力了。最简单的能代替mstime的非heapspay方法了，但坏处是暴力猜测不比heapspray完美到哪去，甚至更差。其次在仅仅有一个任意地址读或者任意地址写得时候可能会只用一个漏洞结合这个绕过各种BT的保护机制（虽然flash的vector已经让任意地址写（不管是相对还是绝对）都变成了一个漏洞绕全部这种节奏，但这种方法总是不嫌多的）。再次，就靠大家的想象力了，参见wushi的“组合漏洞”和yuange的“信息孤岛和联系”论。

说了这么多估计很多人也没耐心看完了，很想像喜闻乐见的四万博士八卦或者爆料给大家提提神，但想了想怎么爆也不如wushi牛的手里一百多个IE漏洞有料，还是算了。最后改编两位老师的话来结尾吧，“每次感觉失去人生意义的时候就默默的走到厕所蹲下，通过思考攻击技术来补充正能量，翻山越岭，克服艰难险阻，搞掂或者搞不掂之后都会陷入一种莫名的空虚之中，感觉找到了人生的意义”。