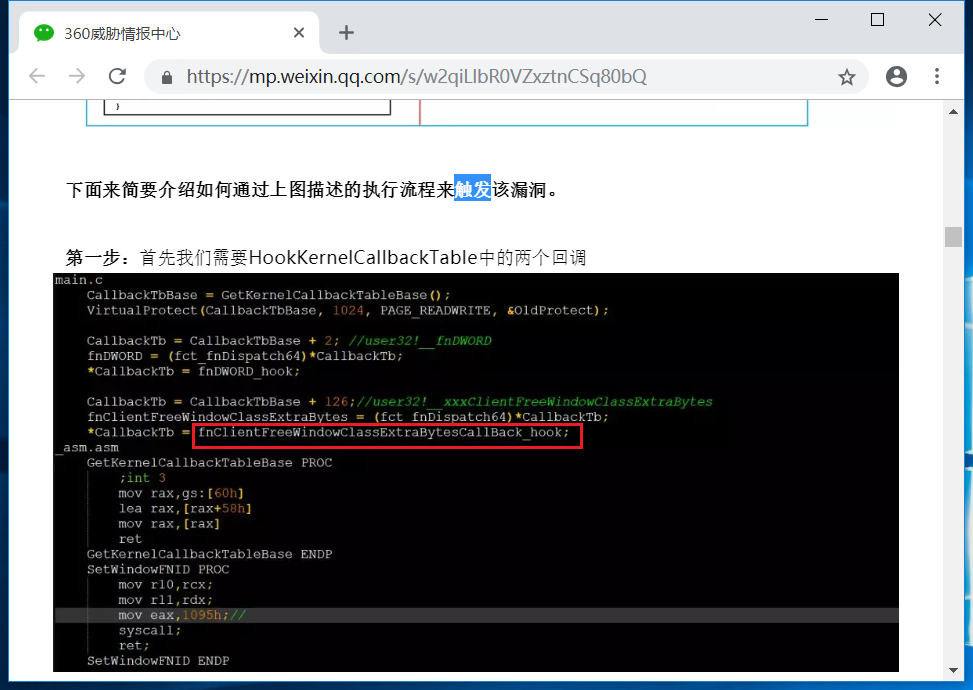
昨晚（2019/1/19 周六）晚上看到某“牛逼”公众号的牛逼文章，号称开发出了CVE-2018-8453的EXP，该EXP可以在win 7到win10 1709版本之间全通用。作为CVE-2018-8453的漏洞分析者真是自愧不如啊！您还是别法律问题了，来，请开源您的EXP代码，让我们开开眼。反正吹牛逼不犯法，我手上有win 2000到window2016所有版本的通杀远程SMB EXP，可以直接GET SHELL（穿透防火墙的），不过鉴于法律问题，我就不公布EXP了，是的，我就是有这么牛逼的东西，但是对不起，我不能发布！

1 在WIN7中， win32k.sys（注：win7中处理图形的是叫做win32k.sys）的xxxDestoryWindow函数根本就没有调用过xxxClientFreeWindowClassExtraBytes，更别提什么回调到用户态以触发漏洞。更牛逼的在于还能WIN7利用成功！在下只能佩服佩服！

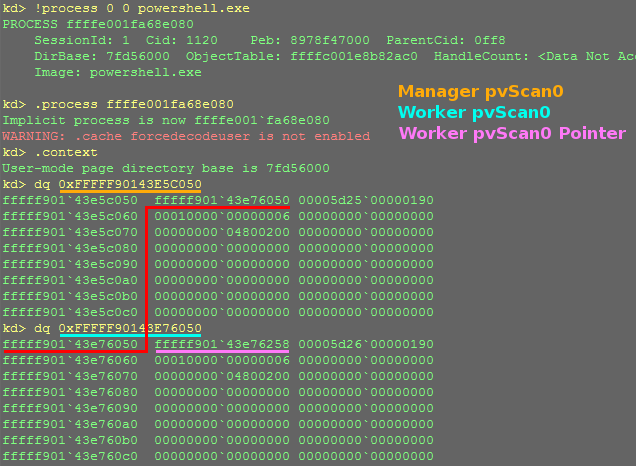


真是厉害，xxxDestoryWindow根本没调用xxxClientFreeWindowClassExtraBytes（没有调用这一点可以看这里：<https://bbs.pediy.com/thread-247444.htm>，问题二中），您怎么触发的二次释放?是在下太笨了，实在惭愧，万望指教下这个HOOK的fnClientFreeWindowClassExtraBytes是干嘛的呀？请您一定要指教一下这个牛逼万能的回调是如何在WIN7下被触发的！在此先行谢过了！睁眼说瞎话！

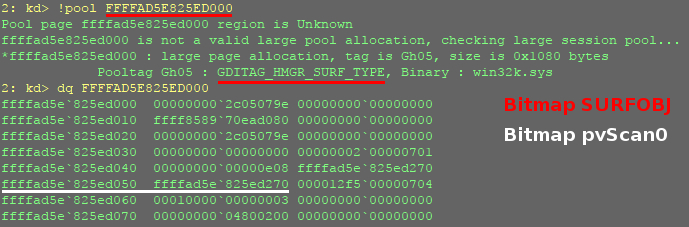
2 您们毕竟厉害，小弟不才，就不说WIN7了，也许您口念口诀就能让WIN7的xxxDesotryWindow调用了这个xxxClientFreeWindowClassExtraBytes。咱说说牛逼的通用WIN 10 1709之前的吧。

截图中，在发送WM\_CANCELMODE消息后，马上申请一个bitmap占用这个原SBTrack的内存。那我是没懂你这SBTrack到底多大？看截图是0x80没错吧？而且下面的数据也显示您是直接覆盖了0xbeefcafe在这里，在下不才，请问您这bitmap对象不需要管理结构吗？：） 您怕是不知道win 10 1609之前版本那bitmap的样子吧？通用？？？您牛逼，怕是我测试用的windows 10是我山寨的吧，我肯定是改了win32kfull.sys来变出来了一个带GDI头的BITMAP对象。我这山寨的就不说了，来看看这两篇文章中的两幅截图：

a <https://bbs.pediy.com/thread-225209.htm>



b: <https://bbs.pediy.com/thread-225296.htm> 注：这个文章里有他们方法的全部介绍，应该是从这里学的，不过哪学的技术不重要。



请告诉我，这俩截图里的pvScan0为何距离bitmap基址这么近的？只相差大概0x200。Bitmap头和bmpbits数据区到底是不是同一次内存申请？为何你截图里没有bitmap结构头？win10 1709通杀?你测试过win 10 1602？？在一个0x80大小的空间内再次申请一个至少0x200大小的内存？睁眼说瞎话！

3 文章最后说了，bitmap对象不需要清理。可能是我小学语文没学好吧，实在看不懂你后面括号里那句话，到底是不需要清理还是不做这步会BSOD而需要清理。姑且认为是不需要清理吧，那你EXP进程还退出吗？如果咱不需要退出这个EXP进程知道系统重启，那在下只能是服了，希望所有用这个EXP的黑客碰到的管理员都是傻子，看不懂进程管理器，另外，那你说的系统重启的时候会BSOD不管了么？我相信您这么牛逼肯定不会做不退出EXP进程的傻逼事，肯定是退出了进程了的，那真是厉害了，一个被释放了数据的bitmap对象，居然在退出时不会BSOD，大神啊！



这里给不明真相的群众说一句：为何不写释放句柄的过程？因为他的版本是微软修复了句柄泄露对象内核地址的版本！想掩盖？

4 提一下，在利用思路里，通过释放对象时减少引用计数来一直减，这个利用思路确实可行。但我想知道，一直利用漏洞来减数字，你这个重占原SBTrack的BITMAP，肯定是每一次减一次数字就会多一个悬挂指针的BITMAP对象吧？不知道你有测试过这个实战性么？一个漏洞中触发至少8次漏洞，不得不说这EXP写的“有艺术”！

5 号称尚未公布EXP？

<https://mp.weixin.qq.com/s/dcbUeegM0BqErtDufOXfoQ>

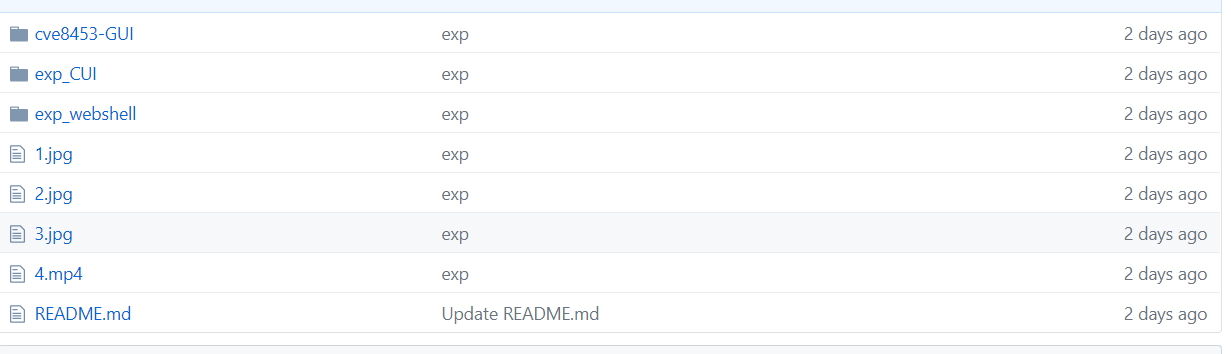
这文章难道是我们黑了微信改的发布时间？

<https://bbs.pediy.com/thread-249021.htm>

这文章是我黑了看雪论坛改的发布时间？帖子内容能编辑，那下面的回复时间也是我编辑的？

<https://github.com/ze0r/cve-2018-8453-exp>

这发布时间也特么是黑客GIT来改的？睁眼说瞎话。



最后再说一句：那么牛逼，win7到win10 1709全通用，请发EXP，实践出真知！让我被EXP打脸，我看到WIN7上可用我道歉！如果还是所谓的法律问题，我只想说：no EXP no bb!