riusksk's blog

Subscribe to feed

攀蟾折桂摄寰宇，摘星揽月御乾坤。踏云踩雾骋宵壤，驱风逐日闯天地。 ------泉哥

<< IDA 自定义结构体快捷键操作方法 | 首页 | Adobe Flash APSB12-22 Sample >>

Heap Spray 技术

日期：2012-10-07 | 分类：软件漏洞

1、堆喷射堆块大小 ≈ 程序堆块分配大小，以减小堆空隙大小。

2、不能使用堆缓存块，否则可能破坏地址的可预测性，可通过申请6块相应大小的堆块来清空缓存。

3、精确定位ROP地址，目标地址如0x0c0c0c0c至堆块数据起始地址的offset = (0x0c0c0c0c - UserPtr（堆数据起始地址）)/2，IE7：0x5FA，IE8：0x5F4/0x5F6，IE9：0x5FC/0x5FE，Firefox9：0x606，可能不同语言版本会存在偏差。

4、不同系统、不同浏览器版本喷射块大小：

XP SP3 – IE7 block = shellcode.substring(2,0x10000-0×21);

XP SP3 – IE8 block = shellcode.substring(2, 0x40000-0×21);

Vista SP2 – IE7 block = shellcode.substring(0, (0x40000-6)/2);

Vista SP2 – IE8 block = shellcode.substring(0, (0x40000-6)/2);

Win7 – IE8 block = shellcode.substring(0, (0x80000-6)/2);

Vista/Win7 – IE9 block = shellcode.substring(0, (0x40000-6)/2);

XP SP3/VISTA SP2/WIN7 - Firefox9 block = shellcode.substring(0, (0x40000-6)/2);

5、Nozzle保护机制（IE）：检测是否存在重复可转换成汇编代码的字段，若存在则阻止其内存申请。

6、BuBBle保护机制（Firefox）：检测JavaScript是否尝试重复申请 NOPs + shellcode (padding + rop chain + shellcode + padding)的内存块，若发现包含这些字段则阻止其内存申请。

7、分配 随机数 + rop + shellcode + 随机数 的堆块，以保证各分配块都是不同的，以此绕过上述保护机制，主要针对IE9。

8、利用随机变量名 + 随机块绕过 Firefox9 的保护。

9、HTML5 Heap Spray：EUSecWest2012上的演讲主题，通杀Chrome、Firefox、IE9和Safari

a、利用canvas标签定义图形，通过脚本控制每个像素的数据再进行喷射；

b、利用Web Worker的多线程功能，加速堆喷射过程，但IE不支持Worker。

最新日志

vim开发环境设置
Hacking Team 武器库研究（六）：Mac OSX Rootkit 技术分析
Hacking Team 武器库研究（五）：Mac OSX 64位 Shellcode 技术分析
Hacking Team 武器库研究（四）：Flash New 0Day（opaqueBackground UAF）
Hacking Team 武器库研究（三）：core-android-audiocapture
Hacking Team 武器库研究（二）：CVE-2015-5119 Flash 0Day
Hacking Team 武器库研究（一）：CVE-2015-0349 Flash ConvolutionFilter UAF
无法声明Activity的问题解决
提取Android内核的方法
绕过最新版 EMET 5.2 保护摘要
全部日志>>

最新评论

Netfairy：很崇拜泉哥--小菜鸟
Prometheus：一样遭遇。前三天发了新日志，直到今天还没能显示，依然审核...
泉哥：已经请求N次了
Joshuabright：你不点审核请求怪谁啦...
9raycat：膜拜
TestGameSafe：有几张相片拍的不错哦...
tingzhou：原来如此。上次没有预约所以没去成的宫崎骏美术馆，下次一定...
泉哥：那机器人是在宫崎骏美术馆里拍的...
风中的纸屑：换wordpress吧
tingzhou：博主可以告诉我那张钢铁机器人的照片是在哪里拍的吗？那是我...

RSS订阅 什么是RSS?
提醒到
FEED QQ邮箱

Tags:
发表于12:36:00 | 编辑 | 分享 0

引用地址： http://www.blogbus.com/public/tb.php/4755401/223258613

发表评论

用户名
密 码

^ 返回顶部