【本周上榜！】看雪论坛精华优秀文章分享与点评

转载

weixin_33674976 于 2018-12-15 17:59:00 发布 85 收藏

他山之石，可以攻玉。好的文章可以给你好的启示和经验，12月即将进入下半场，本周又诞生了哪些好文章呢？

【二进制漏洞】

1、CVE-2017-4901 VMware虚拟机逃逸漏洞分析【Frida Windows实例】

作者：lmyang

入围：**精华文章**

点评：

虚拟机想必大家都用过，它可以让用户可以在一个隔离的环境内运行软件。而这次的VMWare虚拟机漏洞可以让虚拟机客户端在宿主机上执行任意代码。此文的作者用到了当下比较流行的frida工具hook VMWare虚拟机来进行漏洞原理分析，可谓是相当时髦了。

2、CVE-2014-6332学习笔记（精华）

作者：输出全靠吼

入围：**精华文章**

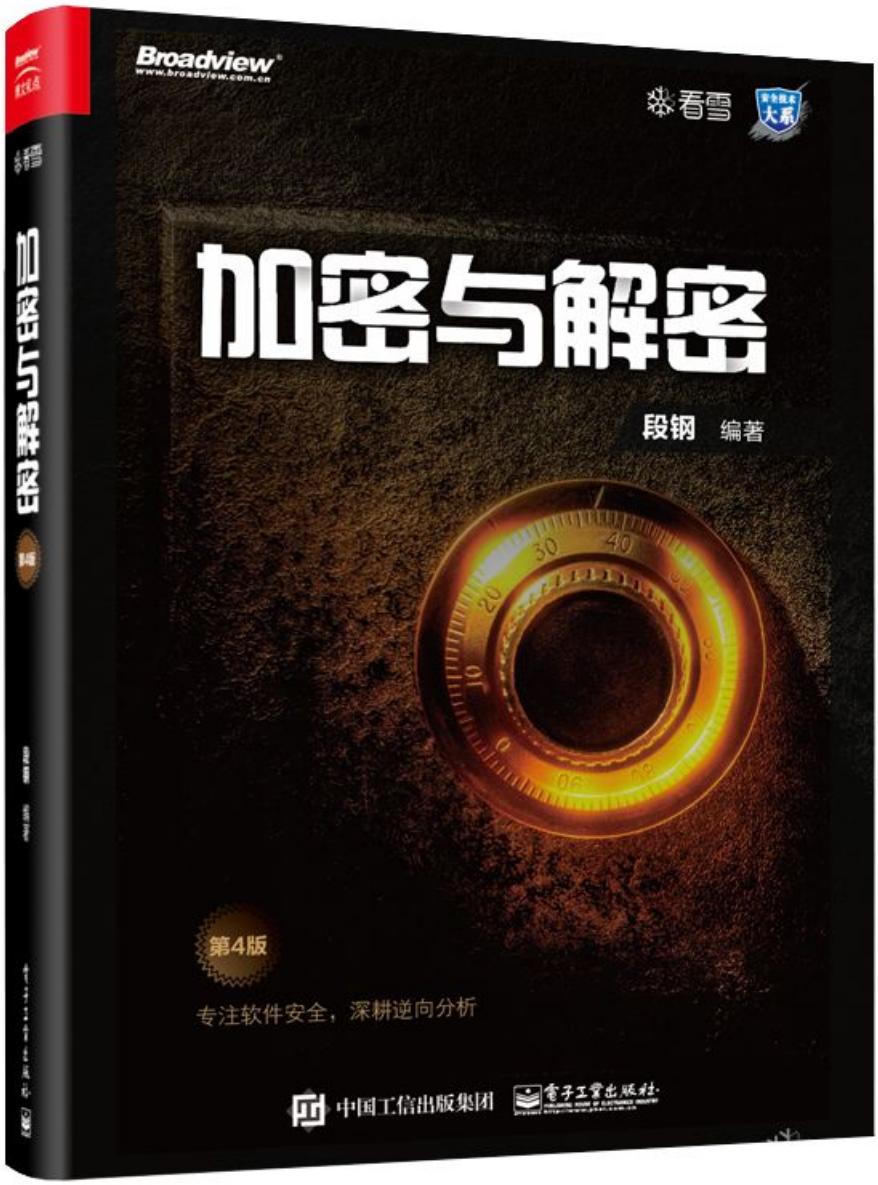
点评：

CVE-2014-6332是微软2014年公布的一个IE浏览器漏洞，影响IE版本为IE3-IE11。作者认为该漏洞是一个存在于IE VBS引擎中的非常经典的数组“越界”的漏洞，并清晰地讲解了定位浏览器漏洞关键代码的方法。

最后16天倒计时开始啦，2018结束之际，我们将会评选出年度最佳原创技术文章，想要赢得丰厚奖品吗？快来看雪论坛留下你的原创文章吧~

签名第4版《加密与解密》+小米AI音响+小米盒子+米家（MIJIA）小米智能插座+1000雪币

正在仓库等你带它走！



点击阅读原文，了解评参赛评选~!

还在等什么，快来投稿吧！

- End -

公众号ID：ikanxue

官方微博：看雪安全

商务合作：wsc@kanxue.com