兴华永恒公司CSO仙果：Flash之殇—漏洞之王Flash Player的末路

原创

csdn业界要闻 于 2017-12-01 15:03:57 发布 825 收藏
文章标签： 安全 Flash 看雪安全开发者峰会

11月18号，2017看雪安全开发者峰会在北京悠唐皇冠假日酒店举行。来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。

7月份，Adobe 公司正式宣布于 2020 年底停止支持 Flash Player，较之“老兵不死，只是逐渐凋零”平添了几分悲情。时光倒回几年前，那时对挖漏洞的人来说， Flash 是再熟悉不过了，每次更新都伴随着一堆 CVE 的修复，此外 Flash 漏洞还备受黑客组织的青睐，被集成到了各种 EK 工具包中。但事物的发展总有其特定规律，无法做到适应的终将被历史所淘汰。看雪论坛二进制漏洞版主，兴华永恒公司CSO仙果在《Flash之殇：漏洞之王Flash Player的末路》主题演讲中，回顾了 Flash 漏洞的繁华往昔及作为漏洞之王的陨落过程。跟着演讲者过一遍 Flash 漏洞的利用思想，也许会为你在研究其它类型漏洞时带来新的灵感。

看雪论坛二进制漏洞版主，兴华永恒公司CSO仙果

> 仙果，看雪论坛二进制漏洞版主，兴华永恒公司CSO。长期从事软件漏洞挖掘、分析、利用方面的工作，具有十年以上的网络安全从业经验。多年在办公处理软件（Office、Adobe Reader、Kingsoft WPS）漏洞方面进行相关的分析利用工作。浏览器漏洞利用方面同样也有相关的分析经验和漏洞利用经验。现致力于网络攻防对抗技术研究，专注软件漏洞的分析与利用。曾在2015年ISC互联网安全大会发表演讲《浏览器漏洞攻防对抗的艺术》；2017 年Kcon 2017 安全大会发表演讲《探索虚拟化技术在漏洞检测中的应用》。

以下为演讲速记：

仙果：刚刚看到一个十几岁的小朋友很认真的在翻简页，感觉到四个字：后生可畏。给自己的感觉是压力很大，心情是越来越紧张。下面开始我们的议题：议题的名字是Flash漏洞之殇，曾经的漏洞之王的末路。大家可以简单跟着我聊一下Flash是怎么流行的，Flash漏洞是怎么回事，又是怎么样利用的，高级的漏洞定义技巧又是什么？大家可以带着这些疑问跟我一块来听一下。

首先自我介绍。我们公司专门做漏洞攻防对抗以及攻防研究的对抗，公司比较久了，来公司已经呆了快十年了，方向是研究漏洞攻防，研究软件漏洞、硬件漏洞以及路由器的漏洞，包括虚拟化的漏洞也会研究，研究的面是比较广的。专注软件漏洞的利用研究以及对抗分析。平时，我其实是比较逗的人，工作中是这样子的，基本上是回到家“修电脑”的人。

我的演讲分五部分，第一是FlashPlayer的往昔盛景，第二是FlashPlayer的成也平台，败也平台。第三，是FlashPlayer漏洞面面观。第四，漏洞缓解措施和对抗，第五，Adobe最后的努力以及放弃。

FlashPlayer的往昔盛景

研究漏洞的人年龄比较大，对这些有印象。像刚刚那位小朋友肯定没有这种印象。首先，为什么会流行？当时的网络很卡，10KB，还是在一个“猫”的阶段。当时很流行一句话，多图杀猫。你的流量很卡，但是如果用FlashPlayer打开非常流量，而且图象不会失真，非常小巧，非常好用。在那个时候它就相当于是一个超人，小巧高效，而且Flash小游戏称霸天下。包括现在很多的页游，就是用Flash进行开发的。

这个图我不知道大家是否有印象，年龄比较大的网虫肯定有印象，闪客帝国和闪吧，我不知道大家是否对这两个还有印象？这对于当时来说非常流行、非常火的两个网站。而且绝大多数是Flash游戏开发以及周边开发都是在这两块发起的。从这个可见，当时FlashPlayer是有多火。我们可以看到它火的一个流程：1996年发布的Flash，1998年开始了Flash3，1994年Flash4，2000年Flash5，包括一直到Flash10的阶段，一直到2008年都是很火的。

通过了十年的发展，它占领了互联网、多媒体的半壁江山，一直到了2005年，是最鼎盛的时候，占有了多媒体浏览98%以上。大家新安装以及XP系统默认安装Flash的组件，不知道大家是否有注意到这个情况。它火了之后，安全人员以及漏洞挖掘人员就会针对Flash进行挖掘，2008年开始一直到今年，2015年是Flash鼎盛之年，2016、2017年也在不断的发展。大家是否注意到漏洞、一些利用包很多都是用的Flash的漏洞，包括APT28，就是这段时间疑似操作美国大选的攻击组织，我们通过分析发现它也使用了Flash的漏洞。

FlashPlayer——成也平台，败也平台

接下来是为什么成也平台，败也平台。截止到2015年Flash早已经从最简单二维矢量网络动画制作软件发展成为跨网络、本地移动设备的应用设计、开发和发布平台。这样就有一个疑问，它为什么会成了一个平台，为什么还要放弃？它就像一个小孩，就像一个婴儿，他承担了一个年轻人，一个中年人，他要承担的份量，这个时候肯定会存在一个问题，它根本就不能承受那么大的重量，而且还发展的那么好，这是一个畸形的发展。

Flash已经成为了一个平台，已经占领了互联网那么大的江山。但是，你在这其中发现了什么？大家能否注意到问题的真正所在？发展那么大，占用那么大的江山，但是它还是浏览器的组建，还是浏览器的插件，它的命掌握在别人手里面，说禁用就禁用，说不用就不用，相当于自己的命根子掌握在别人的手里面一样，这就是它的问题所在。像IE11还支持Flash，其他浏览器的已经不支持Flash。如果浏览器不支持，就会慢慢消亡。

当苹果iOS发布的时候，移动端的iOS已经不再支持Flash，而互联网的发展从现在回头往前看，是移动端者得天下。像iOS和安卓打架诺基亚死掉一样，诺基亚当时多火，但是还是死掉了。Flash放弃了Linux的平台，同时安卓平台也放弃了。很多应用端的游戏，用到的Flash但是已经不算是FlashPlayer了。

FlashPlayer漏洞面面观

再看一下FlashPlayer的攻击面：最鼎盛的时候Flash是支持了很多平台，像Windows、Linux 等等，支持这么多的平台，但是它一旦有了漏洞，它的影响面很大，同时一个漏洞影响多个平台。就像曾经的漏洞之王，Java一样，也是一个跨平台的，一个漏洞影响多个平台，会波及整个互联网。图片解析，这是Flash的源码截取一部分针对图片解析的文件夹，ICO还是比较常建见的，WX是什么？大家知道WX是什么图片？它是具有图片解析的程序，很大可能性是存在漏洞的。正则表达式，这个很奇葩。我们在研究的时候就发现真的是解析出现问题。连正则表达式都会出现问题，这是很奇怪的。视频各式解析，这是它解析FlV格式的漏洞，给我的感觉是什么概念呢？只要是Flash支持的组件，支持的格式，都会存在着漏洞。它就像一个千疮百孔一样，任何人都可以插一脚。ActionScript 3自身，这个不用举例了，很多的漏洞都是自身数据结构上的问题，包括跨域、XSS等等的漏洞。

它的影响面，一个Flash漏洞，攻击者怎么应用这个？它的影响除了在操作系统层面还会顾及到什么层面，这是播放的一个视频，在Word的视频，这个视频是Flash的模式。Flash它影响到了Office，包括一些的Adobe组建都会受影响，还有国内的软件WPS，它也支持Flash的组件。

漏洞缓解措施和对抗

大家可能不太清楚，这是在Flash里面来利用IE漏洞，这样做出来有一个非常大的好处，是攻击者进行漏洞攻防对抗的时候，就有非常大的好处。免杀以及通用性非常大。而且，Flash本身是支持很多操作系统的判断以及浏览器的判断更准确，影响面更大，可以做的事情更多。这是一个漏洞，可以针对W7、W8。只不过这个攻击者没有写相应的XP。操作系统层面，从应用层的层面，包括多功能组合的层面，都会有很大的问题。最奇葩的一个问题是，之前我们测试过的是，PDF的漏洞可以结合多个Flash的漏洞，做到什么程度呢，你只有你想不到，没有做不到。

这是一个演示视频，可能大家看到漏洞演示比较多的是一个网页，计算器弹出来了大家很高兴。下面大家看这一种，打开Flash，操作系统里面安装的软件，补丁就全部泄露出来了，操作系统是Win7，除了Flash是低版本，其他的全都是最新版本。电脑所有安装软件以及补丁全部都有泄露出来，漏洞的威力是非常大的，是很典型文件信息泄露的，是文件读取以及信息泄露的漏洞，这个漏洞可能没有你在本地打开计算器的漏洞危害大，好处是：稳定、好用、高效。在APT攻击流程里面，信息探测占到非常大比例，这个漏洞就是非常好的信息探测的漏洞。你比如说把这个放到局域网里面可以做到什么效果，我不知道大家是否有这样的想法，所有信息全部被泄露了。

不知道大家是否见过这个软件，DoSWF，就是刚刚开始用这个软件进行混淆之后，把它应用到漏洞攻防的EXP混淆的时候，所有操作软件，所有的防御软件全部是绕过的。针对这个检测，安全人员是无从下手的，包括国外的研究人员他们是怎么把这个解析出来，他们是条形加载，解析到流程全部走完之后再从内存里面找到原始有的漏洞放出来，生生的把漏洞扣出来的一个高强度混淆的软件。现在用的比较多的还有另外一个，这个软件是国外用的比较多，SecureSWF，混淆的强度还是比较大的。在2015年的Flash漏洞直线上升，其实荣升了漏洞之王的称号。

Adobe最后的努力以及放弃

再来回顾一下漏洞利用的历史，这是2009年、2010年左右的时候Flash是这样利用的，很粗略、很粗糙，现在回头来看这是非常粗糙的，也是最原始的。这个时候IE只能够做到稳定的控制堆，进行堆风水，Flash能做到什么大家不知道，但是正式测试的时候发现可以很好的进行堆填充。

这个编号是cve-2011-2011，漏洞原因是函数参数导致的问题，三个点来触发的漏洞。牵扯到另外一个问题，很明显的是在进行IE的漏洞，刚才提到了HTML怎么利用的？像刚刚2011一样，有三个点的A，这个利用漏洞是怎么样，直接在Flash里面执行Windows。这是payload，这样执行起来非常简单。在2015年漏洞之后，Adobe针对vector对象引入了Cookie和lenght检测机制，使得Vector的力利用方式被封堵。引入了隔离堆机制，当然还有一些没有加入堆隔离的对象，对象的大小以及不同对象虽然隔离了，但是对于普通对象还是会分到同类的堆里面，包括对象保存的这样机制，延迟释放的这样一些机制。既然是机制，就不可能把每一个对象，因为Flash的对象太复杂了，还是有突出的一些。那怎么办？很明显，Adobe公司已经不要Flash了，它已经把它抛弃了，就像一个很明显的是：爸爸不要你了。

这是我的演讲过程，希望给大家进行漏洞研究方面的交流，谢谢大家！

> 注：本文根据大会主办方提供的速记整理而成，不代表CSDN观点。

2017看雪安全开发者峰会更多精彩内容：

- 2017看雪安全开发者峰会在京召开 共商网络安全保障之策
- 中国信息安全测评中心总工程师王军：用技术实现国家的网络强国梦
- 中国婚博会PHP高级工程师、安全顾问汤青松：浅析Web安全编程
- 威胁猎人产品总监彭巍：业务安全发展趋势及对安全研发的挑战
- 启明星辰ADLab西南团队负责人王东：智能化的安全——设备&应用&ICS
- 自由Android安全研究员陈愉鑫：移动App灰色产业案例分析与防范
- 腾讯反病毒实验室安全研究员杨经宇：开启IoT设备的上帝模式
- 绿盟科技应急响应中心安全研究员邓永凯：那些年，你怎么写总会出现的漏洞
- 腾讯游戏安全高级工程师胡和君：定制化对抗——游戏反外挂的安全实践
- 绿盟科技网络安全攻防实验室安全研究员廖新喜：Java JSON 反序列化之殇
- 阿里安全IoT安全研究团队Leader谢君：如何黑掉无人机