Flash曝出严重安全漏洞 黑客可强制启动

<p>（2008年10月12日北京） 360安全中心今日发出网络安全警报称，一项名为“Clickjacking”的安全问题被曝出，涉及几乎所有的网络应用。其中最严重的就是“Flash强制启动视频”漏洞。利用这一漏洞，黑客可强制启动并完全控制受害网民的摄像头和麦克风，从而对网民个人隐私形成极大的威胁。为此，360安全中心紧急开发了针对该漏洞的专用修复工具（点此下载）。截至本文发稿前，Adobe官方尚未对此漏洞推出安全补丁。 据360安全专家介绍，黑客可以利用“Flash强制启动视频”漏洞，设计一个恶意网页。当网民不慎访问该网页时，就会触发这一漏洞。黑客可以在受害者毫不知情的情况下，强制启动并完全控制其摄像头和麦克风，大肆他人的个人隐私。黑客甚至还可能将通过受害者摄像头和麦克风捕捉到的视、音频资料制作成视频作品在网上进行传播。 据悉，由于Adobe Flash Player软件在互联网上应用极其广泛，而该“Flash强制启动视频”漏洞会影响到Flash软件的绝大多数版本，因而该漏洞已经成为广大网民电脑中非常严重的安全隐患。但截至目前，Adobe官方尚未对此漏洞推出任何安全补丁。 360安全中心紧急开发了针对该漏洞的专用修复工具（点此下载），并强烈建议用户立即使用该工具进行修复，同时建议用户使用360安全卫士为自己的系统打好补丁，以确保尽快远离隐私泄露的威胁。 360安全专家同时提醒广大用户，尽快按如下方案处理： 一、下载使用“Flash强制视频”漏洞工具。 （下载地址：http://dl.360safe.com/360flashvfix.exe） 二、经常使用360安全卫士修复系统及第三方软件漏洞。 三、开启360安全卫士的“网页防漏及恶意网站拦截”功能，及时拦截可能存在风险的网页。 此外，360安全中心建议网民使用360安全浏览器，上网时就能自动屏蔽恶意网址并可智能拦截网页中的恶意代码，使电脑中招的概率降到最低。 _____ _____ 附：新闻背景 一、点击下面链接，观看模拟的黑客攻击动画。（摄像头就这样被打开了…可怕！！） http://baike..360.cn/recomme

nd/4012610/12737516.html 二、“Flash强制启动视频”漏洞的技术内幕。 Clickjacking是OWASP_NYC_AppSec_2008_Conference的一个保密的议题，以下是一些攻击的描叙： 当你访问一个恶意网站的时候，攻击者可以控制你的浏览器对一些链接的访问，这个漏洞影响到几乎所有浏览器以及所有版本的Flash等浏览器相关的第三方软件，除非你使用lynx一类的字符浏览器。 这个漏洞与JavaScript无关，即使你关闭浏览器的JavaScript功能也无能为力。事实上这是浏览器工作原理中的一个缺陷。一个恶意网站能让你在毫不知情的情况下点击任意链接，任意按钮或网站上的任意东西。 该漏洞用到DHTML，使用防frame代码可以保护你不受跨站点攻击，但攻击者仍可以强迫你点击任何链接。你所做的任何点击都被引导到恶意链接上，所以，那些Flash游戏将首当其冲。 最近国外的安全研究人员已经放出了该漏洞的攻击例子，以及部分细节，这种攻击是利用的CSS样式表的网页渲染功能配合IFRAME帧框架页进行的一种钓鱼网页攻击。这个攻击涉及网页设计相关的技巧，步骤是： 1.在第三方站点的网页先用IFRAME引入一个需要攻击的页面,将这个引入的框架页长宽设置成整个浏览窗口的大小。 2.在网页中使用一个CSS滤镜，将整个网页用白色滤镜遮蔽。 3.使用span或div设计一个层伪造一个表单提交按钮、输入框或者链接，然后利用CSS样式表设置层在网页中的位置，遮蔽住需要劫持的网页按钮、输入框或者链接。 攻击者使用这种方法可以制作钓鱼网页，诱导用户在不察觉的情况下，完成一些受攻击WEB程序的敏感操作。 漏洞危害： 攻击者可以制作一个精美的钓鱼网页，让用户在不知不觉中被控制摄像头，或完成密码修改、网银转帐等的恶意操作，给用户造成巨大的损失。

下载本文pdf文件