Swf文件利用姿势学习—【CVE-2017-5494】

phantom0301 / 2017-03-20 13:42:00 / 浏览数 3033 安全技术 漏洞分析 顶(0) 踩(0)

年前学习审计的时候找到的一个CMS的小漏洞，漏洞的发现过程没有什么值得特别介绍的，不过flash的swf文件利用方法之前没有了解过，借此机会学习一下。

0X01 漏洞简介

CVE列表戳这里：

CVE-2017-5494

B2evolution是一个功能丰富的blog管理系统，可以建立多权限的社区管理平台。事实上，它的官网就是用自己的系统搭建的。而在它的6.8.4版本中，允许普通用户在设置头

上图是它在更新版本中的漏洞修复，将swf文件的上传权限设为admin。

0X02 姿势利用

原理性的东西可以参考这一篇文章

https://www.secpulse.com/archives/44299.html

B2evolution使用flowplayer来加载swf文件。
当然这和传统的flash
SWF漏洞不太一样，传统的SWF漏洞是通过阅读服务器上的SWF源码，通过SWF执行时的一些输入参数来实现漏洞利用，而在这里，我们是可以任意上传一个SWF文件，也

通过查阅资料，大致的payload可以有这两种构造方式：
一种是将SWF文件反编译后，直接在其中增加恶意代码
一种是反编译后，通过flash动画制作软件以动作-帧的方式添加脚本，没错，就是古老的网上一搜一大把的flash马的入门玩法。

作为漏洞发掘，我使用第二种方式来快速构造执行文件。

首先从网上下载一段正常的swf视频，反编译导出为fla格式，反编译工具有很多，《Web前端黑客技术揭秘》里提到过SWFScan和swfdump，当然其实不追求HACK仪式感

反编译后，可以使用Macromedia Flash来制作，如图，可以直接使用软件带的函数快速插入功能，与浏览器及网络有关的函数主要说这两个：

- fscommand（ ）可以直接执行命令的函数，不过只在本地有效。
- getURL（ ）
  我用这个函数来实现与Javascript通信，当然，在AS3中它有新函数来代替，但它依然可用。利用这个函数，我们至少可以实现xss和网页跳转两个功能。

在打开的fla文件中添加如下动作，

```
getURL("javascript:alert(1)");
```

然后重新导出当前文件为swf影片，即可上传使用。

0X03 本地实战

下载B2evolution的6.8.4版，按照提示安装完成后，注册任意普通用户，并在数据库中强制完成邮箱认证

任意点击一篇文章，使用评论中的上传功能，上传构造好的swf文件，然后预览相应的文件。

即可成功执行相应命令。

0X04 写在后面

毫无疑问的是，利用上述方法实现的漏洞利用还很有限，如果熟悉ActionScript的话就可以直接敲代码来实现更复杂的逻辑，进而实现更强大的功能，而且这种利用方式如果

上一篇：跨域方法总结 下一篇：MSSQL备份数据库恢复总结

1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板