【独家】一个有意思的APPLE XSS（CVE-2016-7762）的 分析与思考

泳少 / 2017-02-27 06:45:13 / 浏览数 8887 安全技术 技术讨论 顶(0) 踩(0)

文章作者：Avfisher

0x00 前言
应CVE作者的要求帮忙分析一下这个漏洞，实际上这是一个思路比较有意思的Apple
XSS（CVE-2016-7762）。漏洞作者确实脑洞比较大也善于尝试和发掘，这里必须赞一个！

0x01 分析与利用
官方在2017年1月24日发布的安全公告中如下描述：可利用设备：iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later漏洞影响：处理恶意构造的web内容可能会导致XSS攻击漏洞描述：Safari在显示文档时产生此漏洞，且该漏洞已通过修正输入校验被解决了
那么，该漏洞真的如安全公告中所描述的那样被解决了吗？实际上，结果并非如此。
在分析之前，首先先了解一下这到底是个什么漏洞。
POC:

创建一个文档文件，比如：
Word文件（docx）PPT文件（pptx）富文本文件（rtf）

添加一个超链接并插入JS脚本，如：
javascript:alert(document.domain);void(0)javascript:alert(document.cookie);void(0)javascript:alert(location.href);void(0)javascript:x=new Image();x.src="Xss Platform";

3. 上传文件至web服务器然后在Apple设备上使用如下应用打开，如：
   SafariQQ BrowserFirefox BrowserGoogle BrowserQQ客户端微信客户端支付宝客户端
4. 点击文档文件中的超链接，上述JS脚本将会被执行从而造成了XSS漏洞

效果图如下：

回顾一下上面的POC，发现其实该漏洞不仅仅存在于Safari中而是普遍存在于使用了WebKit的APP中。
我们都知道，iOS
APP要想像浏览器一样可以显示web内容，那么就必须使用WebKit。这是因为WebKit提供了一系列的类用于实现web页面展示，以及浏览器功能。而其中的WKWebView
该漏洞单从利用的角度来说还是比较鸡肋的，因为漏洞的触发必须依赖于用户点击文档中的超链接，笔者可以想到的可能的利用场景如下：攻击者上传了一个包含了恶意JS的
0x02 思考
这个XSS漏洞本身其实并没有太多的技术含量或者技巧，但是在挖掘思路上却是很有意思且值得思考的。漏洞作者并没有将利用js直接插入至web页面本身，而是巧妙地利用

0x03 作者语录
其实这个漏洞的产生早在12年的时候就有类似的案例了，目前Apple修复了该漏洞后我还继续做了些深入的研究，其实不仅仅局限于javascript的协议，当然还可以用上sms
Security Response Center的一些帮助！

0x04 参考
https://support.apple.com/en-us/HT207422
https://developer.apple.com/reference/webkit
https://developer.apple.com/reference/webkit/wkwebview
https://developer.apple.com/reference/uikit/uiwebview

上一篇：浅谈Discuz插件代码安全（内附... 下一篇：从SHAttered事件谈安全

1. 16 条回复


紫霞仙子 2017-02-27 06:52:11

cve泳

0 回复Ta


影子 2017-02-27 06:53:55

cve 泳师傅 不愧是我大师傅

0 回复Ta


zirvana 2017-02-27 06:58:27

厉害

0 回复Ta


hades 2017-02-27 07:00:07

改天可以看看富文本文件（rtf）的一些东西 哈哈

0 回复Ta


hellotest 2017-02-27 07:00:13

cve 泳！

0 回复Ta


root 2017-02-27 07:33:22

cve泳

0 回复Ta


安全小飞侠 2017-02-27 08:40:24

cve泳

0 回复Ta


xiaopigfly 2017-02-27 09:00:06

cve泳

0 回复Ta


hades 2017-02-27 09:28:24

iOS下的URLScheme存在几个特点：

1. iOS 下URL Schemes全局有效且只需安装app即可生效。
2. iOS下的URL Schemes的链接会被UITextView或者UIWebView的Detection Links属性识别为链接。
   我们先看第2点的具体处理机制"UIWebView的Detection Links属性识别为链接"，也就是说你输入的任何URL Scheme连接都会被解析html里的a标签的调用：

```
scheme:// –> <a … href="scheme://"> … </a >
```

对XSS漏洞很熟悉的同学，很可能就会想到2个方向：

1. 通过双引号闭合使用事件来执行js 经过测试在上引号出现在scheme里不会被识别，所以这个思路不通。
2. 利用javascript:// 伪协议执行js
   在主流的浏览器内核有2种方法调用，最常见的方法：

```
<a href='javascript:alert(1)'>knownsec 404</a>
```

还有另外一种格式方法很少有人正规使用：

```
<a href='javascript://%0a%0dalert(1)'>knownsec 404</a>
```

注意:与//的区别，也就是这种非常见的方式导致了很多程序的漏洞，比如前面曝光的iMessage的XSS漏洞（CVE-2016-1764）
所以这个"BadURLScheme"就是javascript了，我们回到前面提到的iOS下的URLScheme的第一个特点，当用户安装了一个注册了javascript这个URL Scheme的任意app后，如果其他的app里使用了UIWebView并且设置了Detection Links属性识别，那么在这些app里输入文本内容：

```
javascript://%0a%0dalert(1)
```

会被Detection Links属性解析为<a>调用：

```
<a dir="ltr" href="javascript://%0a%0dalert(1)" x-apple-data-detectors="true" x-apple-data-detectors-type="link" x-apple-da
```

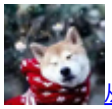
成而导致这些app的XSS漏洞。

0 回复Ta


r4bb1t_ 2017-02-27 09:57:07

冰总发东西的格式十分让人舒心

0 回复Ta

 从容 2017-02-27 12:02:54

xss payload嵌入到二维码也值得研究，比如支付宝扫描嵌入了mailto:的二维码就会自动跳转，之前好像有类似的扫码xss案例。

0 回复Ta

 hades 2017-02-27 13:13:07

第一次听说这个，改天从容也来分享分享

0 回复Ta

 泳少 2017-02-28 01:09:57

有链接吗？发来看看

0 回复Ta

 紫霞仙子 2017-02-28 01:55:02

改天把你的分析也发来啊

0 回复Ta

 泳少 2017-02-28 02:01:05

你说的这个我看了，挺有意思的。啥协议都不识别。就是别这个mailto:xxx@a.com

0 回复Ta


xiaopigfly 2017-02-28 02:40:51

泳师傅厉害了

0 回复Ta

登录 后跟帖

先知社区

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