ZipperDown漏洞简单分析及防护

先知 / 2018-05-16 15:10:00 / 浏览数 4271 安全技术 漏洞分析 顶(0) 踩(0)

蒸米，白小龙 @ 阿里基础安全研究
授权发布

0x00 序

盘古实验室在针对不同客户的iOS应用安全审计过程中，发现了一类通用的安全漏洞。该漏洞被发布在了[1]。经过盘古的分析，确认微博、陌陌、网易云音乐、QQ音乐、快

根据漏洞名称大概可以猜测出与zip文件有关，查询iOS上与解压相关资料可以看到，iOS并没有提供官方的unzip API函数，基本上现有的iOS app都是使用的SSZipArchive或ziparchive这两个第三方库来实现解压的功能。随后根据盘古在SSZipArchive项目的issue中提交的漏洞报告[2]可以大概确定漏洞原理是：使应用下载了恶意的zip文件，并且使用ziparchive库解压，利用漏洞可以做到app container目录下的任意文件覆盖，如果覆盖了应用重要的文件会造成应用崩溃（DOS），如果覆盖了app的hotpatch文件则会造成代码执行。

0x01 构造恶意的ZIP文件（POC）

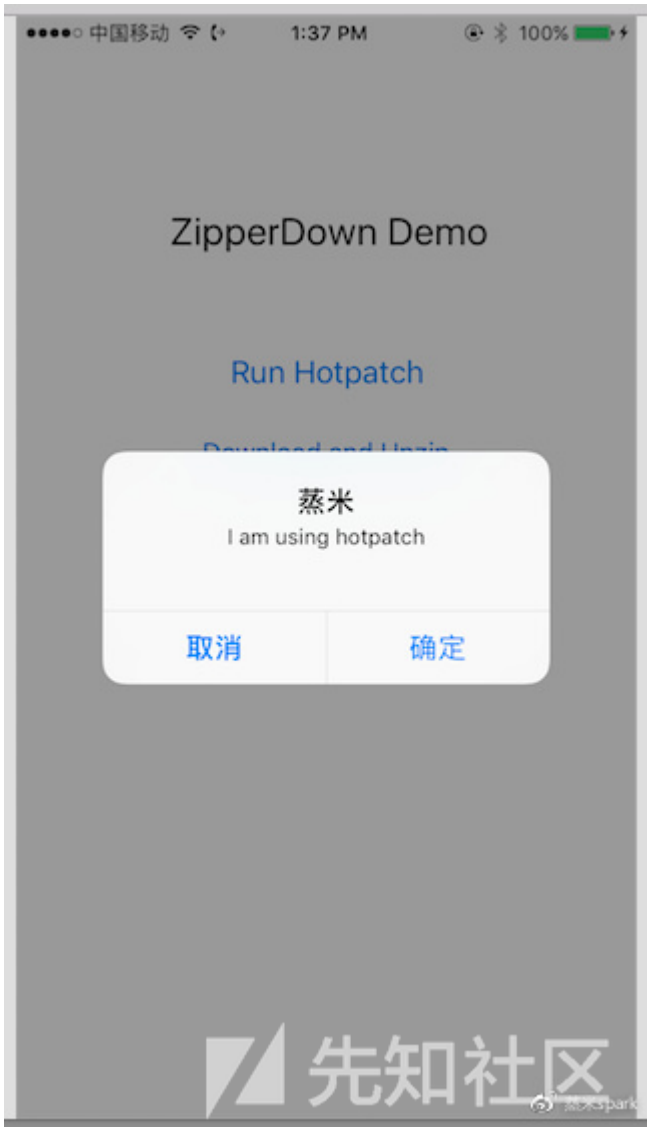
（因为很多app并没有修复该漏洞，因此POC暂不公布，想要了解细节的同学可以联系阿里巴巴SRC）

0x02 复现攻击

正常情况下，应用会在启动或者某些情况下会执行hotpatch的js脚本。在我们用来demo的应用中需要点击一下"Run Hotpatch"来运行js脚本：

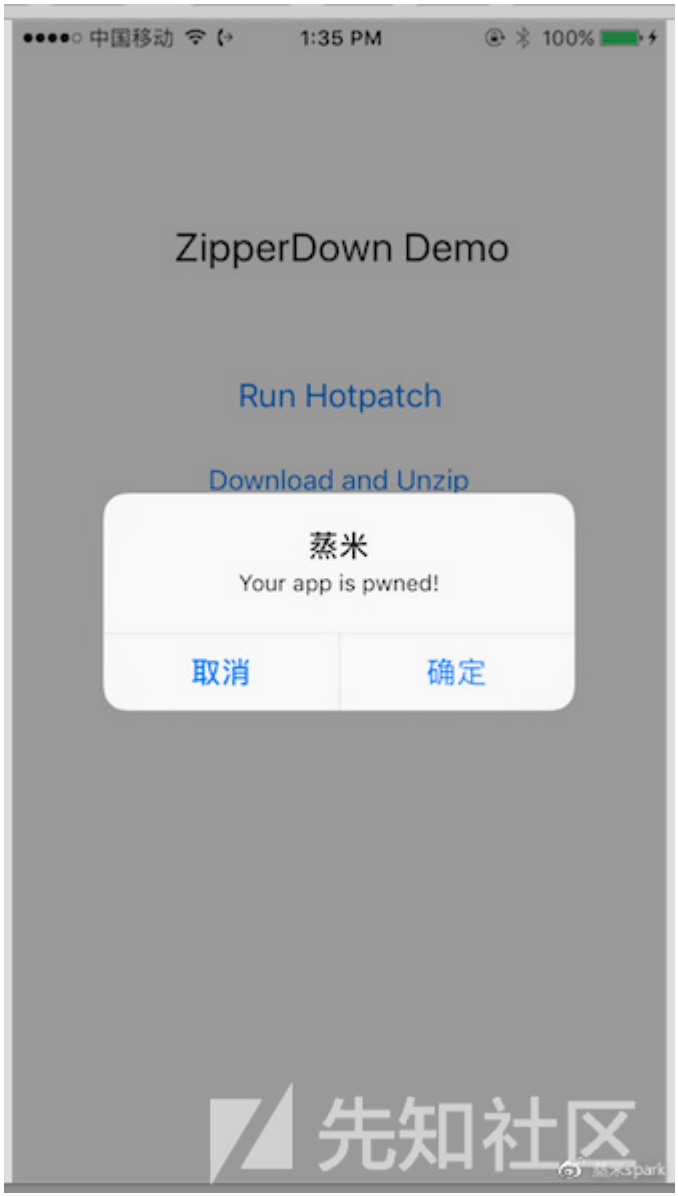
点击完后，应用会加载自己目录下的"/Library/Caches/hotpatch/patch.js"并执行：

```
mzheng-iphone:/var/mobile/Containers/Data/Application/B26B915E-C85A-4F66-A2C1-A2C26E3A05DE/Library/Caches root# ls
download/  hotpatch/
mzheng-iphone:/var/mobile/Containers/Data/Application/B26B915E-C85A-4F66-A2C1-A2C26E3A05DE/Library/Caches root# ls hotpatch/
patch.js*
```

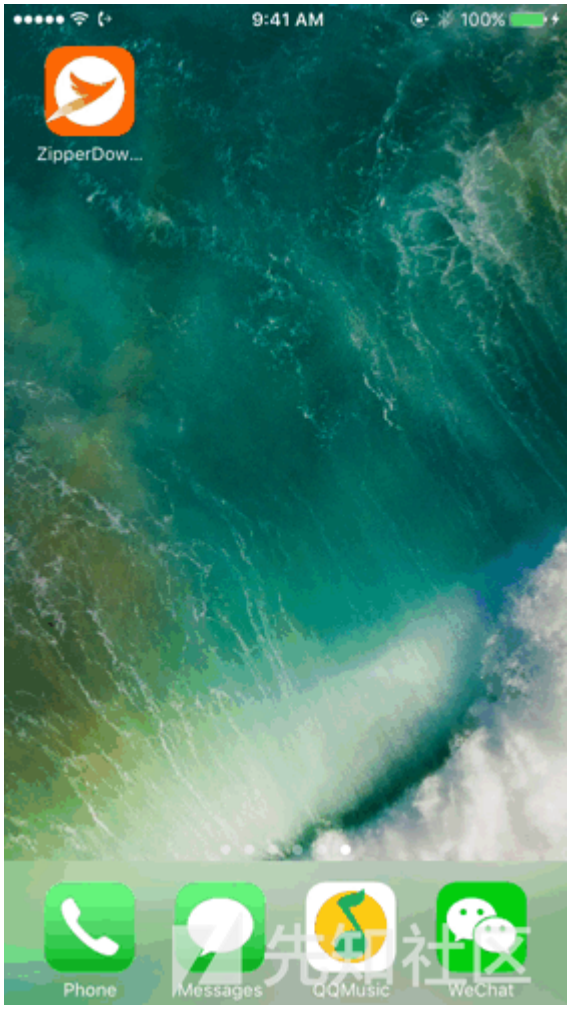


随后我们点击“Download and
Unzip”，应用会通过http下载一个zip包到本地，并使用SSZipArchive库进行解压，如果我们采用DNS劫持将正常的zip包替换为恶意的zip包的话，虽然程序会将zip解压到c

```
mzheng-iphone:/var/mobile/Containers/Data/Application/B26B915E-C85A-4F66-A2C1-A2C26E3A05DE/Library/Caches root# ls
Snapshots/  download/  hotpatch/
mzheng-iphone:/var/mobile/Containers/Data/Application/B26B915E-C85A-4F66-A2C1-A2C26E3A05DE/Library/Caches root# ls ./download/
test.zip
mzheng-iphone:/var/mobile/Containers/Data/Application/B26B915E-C85A-4F66-A2C1-A2C26E3A05DE/Library/Cache
anythingwewant  patch.js*
```



演示DEMO：https://v.qq.com/x/page/a0655dtirv7.html



0x03 防御方案

最完整的解决方案是对SSZipArchive库进行修补，在解压函数：

```
+ (BOOL)unzipFileAtPath:(NSString *)path toDestination:(NSString *)destination preserveAttributes:(BOOL)preserveAttributes ove
```

中对最终解压的strPath进行检测，如果出现可能造成目录穿越的"../"字符串时进行拦截。

另外，Hotpatch包除了传输过程中要加密外，在本地也需要加密保存，并且运行前做完整性校验。虽然漏洞覆盖某些重要的文件可能会造成拒绝服务攻击，但至少不会造成

0x04 总结

正如JSPatch的作者bang所讲的："攻击条件：1.APP用了ZipArchive 2.原APP下发的某个zip包传输过程没加密，zip包也没加密
3.原APP使用了JSPatch或其他执行引擎，且本地脚本没有加密，只要把脚本放指定目录即可执行
4.用户连上第三方wifi遭受攻击。恰好视频中的微博满足这些苛刻条件。危害很小，能被攻击的APP也很少。"

因此，能够造成代码执行的应用可能没有想象中那么多，但黑客依然有可能利用任意文件覆盖的漏洞能力对应用进行攻击，造成意想不到的效果。

0x05 参考资料

https://zipperdown.org
https://github.com/ZipArchive/ZipArchive/issues/453

上一篇：Spring Data Redis... 下一篇：【CVE-2018-1259】XX...
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