南明离火
移动应用检测平台

ANDROID 静态分析报告

APhone • v1.0

分析日期: 2024-06-04 16:05:50

应用概览

文件名称:	APhone-v1.0.apk
文件大小:	1.83MB
应用名称:	APhone
软件包名:	com.aphone.app
主活动:	com.aphone.app.SplashActivity
版本号:	1.0
最小SDK:	21
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	42/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	2d0418e5849ad4a22c7312992fb3b760
SHA1:	4ca39563e92b106a741c8ad4572bd3e0c1f7160f
SHA256:	7861284fbc7b6911f3790c88f5[illegible]3052263888c9165eac4b59d9adcb577e05f6b

分析结果严重性分布

高危	中危	信息	安全	关注
2	1	1	1	1

四大组件导出状态统计

Activity组件：3个，其中export的有：1个
Service组件：1个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=SG, ST=Singapore, L=Singapore, O=APHONE PTE. LTD., OU=APHONE, CN=APHONE
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-09 07:40:15+00:00
有效期至: 2049-05-03 07:40:15+00:00
发行人: C=SG, ST=Singapore, L=Singapore, O=APHONE PTE. LTD., OU=APHONE, CN=APHONE
序列号: 0x7376850a
哈希算法: sha256
证书MD5: e638f75465d6b5cf701046affb4f2ed7
证书SHA1: 88b47845c37450eeccb8ca9e09bbdac737d7de73
证书SHA256: ef5c67755cef80311aab631555922431f72bf6a16b598e154d143dbd80a676a5
证书SHA512:
7e410fe63bf703d08a001eb11de2c4feecc41b04c76331efe84f67f7dc7fbf8db4fb572e010e0c41767e8e7bfb0cb7a3456c0[illegible]3330f811cdef9ec4064bcf

公钥算法: rsa
密钥长度: 2048
指纹: e45dc98160bcc6abd0ca40d1d261902adaeb77ef4857b76c974a630fdb67e5b2
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

本报告由南明离火移动安全分析平台生成

Manifest 配置安全分析

高危: **0** | 警告: **0** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。

代码安全漏洞检测

高危: **1** | 警告: **1** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
2	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
3	应用程序记录日志信息，不得将敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.READ_PHONE_STATE android.permission.GET_TASKS
其它常用权限	4/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
app.aphone.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://app.aphone.com/uq78j6tve1xgoytsm0eh?utm_source=website	com/aphone/app/WebActivity.java
• https://app.aphone.com/uq78j6tve1xgoytsm0eh?utm_source=website • https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047 • https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041 • https://debugtbs.qq.com?10000 • https://mdc.html5.qq.com/mh?channel_id=50079&u= • https://cfg.imtt.qq.com/tbs?v=2&mk= • https://debugx5.qq.com • https://tbsrecovery.imtt.qq.com/getconfig • https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079 • https://debugtbs.qq.com • www.qq.com • https://mqqad.html5.qq.com/adjs • https://pms.mb.qq.com/rsp204 • https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_debugplugin_debugplugin.tbs • 4.3.0.67 • file:unexpect	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。