南明离火
移动应用检测平台

ANDROID 静态分析报告

批八字算命 • v1.87

分析日期: 2024-05-28 23:01:27

应用概览

文件名称:	批八字算命_1.87(1).apk
文件大小:	5.07MB
应用名称:	批八字算命
软件包名:	com.nfzhouyi.pibazi
主活动:	com.nfzhouyi.pibazi.splash_activity
版本号:	1.87
最小SDK:	26
目标SDK:	33
加固信息:	360加固 加固
应用程序安全分数:	64/100 (低风险)
杀软检测:	AI评估：安全
MD5:	d205ca2d7b707b90a989dec5e19293ec
SHA1:	94f5ac492350304f501b73f760bbce1101ba5077
SHA256:	f1367ffff46443eb569f81ac0467b2...751e6881148f1467d6cae1a5d1005b62

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	11	1	1

四大组件导出状态统计

Activity组件：13个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：0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=511495, ST=guangdong, L=guagnzhou, O=nanfang zhouyi, OU=nfzhouyi, CN=fang nan
签名算法: rsassa_pkcs1v15
有效期自: 2019-02-10 02:29:13+00:00
有效期至: 2044-02-04 02:29:13+00:00
发行人: C=511495, ST=guangdong, L=guagnzhou, O=nanfang zhouyi, OU=nfzhouyi, CN=fang nan
序列号: 0x2de73b87
哈希算法: sha256
证书MD5: 08175b1cac5977a9081f8c825239b0b4
证书SHA1: 789f9a582b06a96d004c18ba3d53bbeef6744bb4
证书SHA256: 591ff0d30e57c51c7aee3c9e124dcafb361dc0257bb64ee6bb43574396c0640d
证书SHA512:
1ab43cc6ef07268a61e477aedc1bb409927b879e955abf342e2aa44bce0b4317271e96ee3af7822eec02c96b94f5f0945599a4cc31efcfc7ddfc1bde7b592e4a

公钥算法: rsa
密钥长度: 2048
指纹: e60fb2785f84a8f88e983cb35266f307096fab6510b0d37d866bb43e1da18a22
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.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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。

网络通信安全风险分析

序号	范围	严重级别	描述

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

Manifest 配置安全分析

高危: **0** | 警告: **1** | 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存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

代码安全漏洞检测

高危: **0** | 警告: **3** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	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
2	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
3	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
4	SHA-1是已知存在哈希冲突的算法	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	4/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

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
www.nfbazi.com	安全	是	**IP地址:** 59.110.54.254 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.nfbazi.com/cesoft/nfcesoft.htm	com/nfzhouyi/pibazi/textShareActivity.java
• http://www.nfbazi.com/cesoft/android/android_version80.png' • http://www.nfbazi.com/download/android/an_paibazi.apk • http://www.nfbazi.com/'	com/nfzhouyi/pibazi/webshow.java
• http://www.nfbazi.com/download/android/an_pibazi80.apk' • http://www.nfbazi.com/download/android/an_zonghepp80.apk' • http://www.nfbazi.com/download/android/an_qimen80.apk' • http://www.nfbazi.com/download/android/an_jiajufsh80.apk' • http://www.nfbazi.com/download/android/an_liuyaoduangua80.apk' • http://www.nfbazi.com/download/android/an_jinkoujue80.apk' • http://www.nfbazi.com/' • http://www.nfbazi.com • http://www.nfbazi.com/download/android/an_calendar80.apk' • http://www.nfbazi.com/cesoft/android/android_version80.png' • http://www.nfbazi.com/download/android/an_proname80.apk' • http://www.nfbazi.com/download/android/an_baziysh80.apk' • http://www.nfbazi.com/download/android/an_xuankong80.apk' • http://www.nfbazi.com/download/android/an_paibazi80.apk' • http://www.nfbazi.com/download/android/an_liuyaopaipan80.apk' • http://www.nfbazi.com/download/android/an_zeji80.apk' • http://www.nfbazi.com/download/android/an_bazimeiri80.apk'	v/a.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。

邮箱地址敏感信息提取

EMAIL	源码文件

416532971@qq.com nfbazi@21cn.com	v/a.java

免责声明及风险提示: