南明离火
移动应用检测平台

ANDROID 静态分析报告

Face Mood Scanner v4.2

分析日期: 2024-07-27 10:04:58

应用概览

文件名称:	0a7695a7a6c27bdf7e3acd77136642589a28de08b14a81328a39bd3ab5fd095d.apk
文件大小:	1.22MB
应用名称:	Face Mood Scanner
软件包名:	com.wideapps.android.facemoodscanner
主活动:	.FaceMoodScannerActivity
版本号:	4.2
最小SDK:	3
目标SDK:	14
加固信息:	未加壳
应用程序安全分数:	38/100 (高风险)
跟踪器检测:	3/432
杀软检测:	29 个杀毒软件报毒
MD5:	c7e7bd5f0912c09850bc3521ea121e9c
SHA1:	75dd48e5cd7a88a99a8b5c784[illegible]1465c6edf
SHA256:	a650e05245a814cd3663a8[illegible]0121664b8f7f8c9[illegible]c46464b8b53aae1c

分析结果严重性分布

高危	中危	信息	安全	关注
3	10	1	0	0

四大组件导出状态统计

Activity组件：5个，其中export的有：0个
Service组件：2个，其中export的有：1个
Receiver组件：5个，其中export的有：1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: False
v3 签名: False
v4 签名: False
主题: C=CN, ST=zj, L=hz, O=hdu, OU=hud, CN=wu
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-11 04:16:58+00:00
有效期至: 2079-03-15 04:16:58+00:00
发行人: C=CN, ST=zj, L=hz, O=hdu, OU=hud, CN=wu
序列号: 0x1e35b2a
哈希算法: sha256
证书MD5: 9c61ac9492cd7ad0a59d5783bb627be6
证书SHA1: 076c8130e6a469cbbf9c22f7573b5e1a5fb5f353
证书SHA256: 6056da6dd3fcde56b8d27390867b625cccf6cd6de72f288e469f360991067aee
证书SHA512:
201f718be189c71aba352121a6661e4623b3899bb00ebb90f7dd2954452af3d1b90fc58222373f682105615d7fb7f2e0880e0d194097ec4341920fb246c1ceaf

主题: CN=asanka
签名算法: rsassa_pkcs1v15
有效期自: 2012-02-10 02:32:39+00:00
有效期至: 3011-06-13 02:32:39+00:00
发行人: CN=asanka
序列号: 0x4f3481c7
哈希算法: sha1
证书MD5: c9cfc795c5d67c9d8862634df887203b
证书SHA1: 98bae6b2118ec4a07c4434fb10c110fc01ca0830
证书SHA256: 6e598b94072a9f616e12383f08a0e4f6f0038c505f1061124ae94414926d9ceb
证书SHA512:
4c22c99d60c8823c25df683e8840e5e167df0b14a80c27938de9522ddf3d573661c430bf80ca36e7ab373ef85626[illegible]3634bc2ac669e6b0f6d56abb0e1762e7

找到 2 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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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。
com.android.browser.permission.READ_HISTORY_BOOKMARKS	危险	获取自带浏览器上网记录	恶意代码可有利用此权限窃取用户的上网记录和书签。
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	危险	修改自带浏览器上网记录	恶意代码可有利用此权限篡改用户的上网记录和书签。

android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
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。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.motorola.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.motorola.dlauncher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.fede.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.lge.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
org.adw.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.motorola.launcher.permission.INSTALL_SHORTCUT	未知	未知权限	来自 android 引用的未知权限。
com.motorola.dlauncher.permission.INSTALL_SHORTCUT	未知	未知权限	来自 android 引用的未知权限。
com.lge.launcher.permission.INSTALL_SHORTCUT	未知	未知权限	来自 android 引用的未知权限。

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: **1** | 警告: **0** | 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

应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **0** | 警告: **3** | 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 1.5, [minSdk=3]	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。
3	Broadcast Receiver (com.wideapps.android.facemoodscanner.BootReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问，intent-filter的存在表明这个Broadcast Receiver是显式导出的。
4	Service (com.airpush.android.PushService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问，intent-filter的存在表明这个Service是显式导出的。

代码安全漏洞检测

高危: **2** | 警告: **5** | 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泄露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	该文件是World Readable。任何应用程序都可以读取文件	高危	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	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

4	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
5	该文件是World Writable。任何应用程序都可以写入文件	高危	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
6	MD5是已知存在哈希冲突的弱哈希	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
7	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	SHA-1是已知存在哈希冲突的弱哈希	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	7/30	android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_WIFI_STATE

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
ad.leadboltads.net	安全	否	**IP地址:** 82.192.82.227 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.188.238 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
beta.airpush.com	安全	否	No Geolocation information available.
www.searchmobileonline.com	安全	否	**IP地址:** 142.250.188.238 **国家:** 美利坚合众国 **地区:** 新泽西州 **城市:** 克利夫顿 **纬度:** 40.858585 **经度:** -74.163605 **查看:** Google 地图
ad.leadbolt.net	安全	否	No Geolocation information available.
api.airpush.com	安全	否	**IP地址:** 142.0.206.124 **国家:** 美利坚合众国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.786339 **经度:** -96.820503 **查看:** Google 地图
ad.leadboltapps.net	安全	否	**IP地址:** 172.234.222.138 **国家:** 美利坚合众国 **地区:** 伊利诺伊州 **城市:** 芝加哥 **纬度:** 41.875771 **经度:** -87.620605 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://api.airpush.com/v2/api.php • http://api.airpush.com/testmsg2.php	com/airpush/android/HttpPostData.java

• http://api.airpush.com/v2/api.php?apikey= • http://api.airpush.com/model/user/getappinfo.php?packagename=	com/airpush/android/SetPreferences.java
• https://play.google.com/store/apps/details?id=com.wideapps.android.facemoodscanner • http://ad.leadboltads.net/show_app_wall?section_id=549285763	com/wideapps/android/facemoodscanner/ResultActivity.java
• http://api.airpush.com/redirect.php?market=	com/airpush/android/DeliveryReceiver.java
• http://beta.airpush.com/images/adsthumbnail/48.png • http://api.airpush.com/redirect.php?market=	com/airpush/android/PushService.java
• http://api.airpush.com/320x350.jpg • http://api.airpush.com/testicon.php	com/airpush/android/Airpush.java
• http://ad.leadboltads.net/show_app_wall?section_id=549285763	com/wideapps/android/facemoodscanner/FaceMoodScannerActivity.java
• http://api.airpush.com/v2/api.php • http://api.airpush.com/testmsg2.php	com/airpush/android/Constants.java
• http://ad.leadbolt.net • http://market.android.com • http://ad.leadboltapps.net • https://market.android.com	com/Leadbolt/AdController.java
• http://api.airpush.com/model/user/getappinfo.php?packagename=	com/airpush/android/UserDetailsReceiver.java
• http://api.airpush.com/model/user/getappinfo.php?packagename=	com/airpush/android/MessageReceiver.java
• http://www.searchmobileonline.com/{$category$}?sourceid=7&q={$query$}	com/apperhand/device/android/AndroidSDKProvider.java
• http://api.airpush.com/v2/api.php • http://api.airpush.com/api.php	com/airpush/android/PushAds.java
• http://api.airpush.com/v2/api.php?apikey= • https://play.google.com/store/apps/details?id=com.wideapps.android.facemoodscanner • http://api.airpush.com/testmsg2.php • http://ad.leadboltapps.net • http://api.airpush.com/api.php • http://ad.leadbolt.net • http://beta.airpush.com/images/adsthumbnail/48.png • http://api.airpush.com/v2/api.php • http://market.android.com • http://api.airpush.com/model/user/getappinfo.php?packagename= • http://api.airpush.com/redirect.php?market= • http://api.airpush.com/testicon.php • http://www.searchmobileonline.com/{$category$}?sourceid=7&q={$query$} • http://api.airpush.com/320x350.jpg • http://ad.leadboltads.net/show_app_wall?section_id=549285763 • https://market.android.com	自研引擎-S

邮箱地址敏感信息提取

EMAIL	源码文件
asankae06@gmail.com	com/wideapps/android/facemoodscanner/ResultActivity.java

asankae06@gmail.com	com/wideapps/android/facemoodscanner/FaceMoodScannerActivity.java
asankae06@gmail.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Airpush	Advertisement	https://reports.exodus-privacy.eu.org/trackers/337
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

敏感凭证泄露检测

可能的密钥
"ga_api_key" : "UA-31924598-1"
CRoQAlVGS1keGVoEHgRLEBoOGRdLEUE+agQtJzsiJj8tABJOHhYdGwYHQQU=

免责声明及风险提示: