南明离火
移动应用检测平台

ANDROID 静态分析报告

爱 神 • v5.0.2

分析日期: 2024-05-22 16:18:06

应用概览

文件名称:	184bc076241730093fb6fe5d794a6f3f809aa7cd6db14b2f0ce67c16c5922604.apk
文件大小:	40.52MB
应用名称:	爱 神
软件包名:	com.ttsgrwzued.dufnchmnnq
主活动:	com.QBEIFZyG.HLsGcRHq.rssdbxoUQuKHZAve
版本号:	5.0.2
最小SDK:	16
目标SDK:	27
加固信息:	资源混淆
应用程序安全分数:	57/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	02bc654f5c7043f4ae7b7f49c01e7131
SHA1:	fdb52adcc48fb2ba09e950eeff2b839b25c83b93
SHA256:	184bc076241730093fb6fe5d794a6f3f809aa7cd6db14b2f0ce67c16c5922604

分析结果严重性分布

高危	中危	信息	安全	关注
0	8	1	1	1

四大组件导出状态统计

Activity组件：8个，其中export的有：0个
Service组件：2个，其中export的有：0个
Receiver组件：4个，其中export的有：2个
Provider组件：4个，其中export的有：4个

应用签名证书信息

二进制文件已签名
v1 签名: False
v2 签名: True

v3 签名: False
v4 签名: False
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-30 19:17:45+00:00
有效期至: 2078-10-02 19:17:45+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x2fe7ec97eba0ea98
哈希算法: sha256
证书MD5: 7cf080ee93d627f5ebd94b71b79aa433
证书SHA1: 8df83e1843fe87a389588586978e59c7ea931182
证书SHA256: 98d9855558326ba1c3237bf7a0a5c3bb0c3b8e81e3c148757ee3f5a0ec5318c4
证书SHA512:
eb15e3192e12718f10a4f0e1992923c1141b79fb98d9b847c6c72d3fdb460767b1b6dafebb8d80f99dea97b93935bf2068089c17b081c2eb7f49141346c09117

公钥算法: rsa
密钥长度: 2048
指纹: 59eeff9a6e2834f59a4543cd6c58cc3a734bff07ff3e256773e3aace225ad7a8
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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。
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.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。
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。
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForegr ound，用于podcast播放（推送悬浮播放，锁屏播放）
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_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.ttsgrwzued.dufnchmnnq.DYNAMIC_RECEIVER_ NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。

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: **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

Manifest 配置安全分析

高危: **0** | 警告: **7** | 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 4.1-4.1.2 [minSdk=16]	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	Content Provider (com.QBEIFZyG.HLsGcRHq.SfNJEZbMEGlDMDWm) 如果应用程序在API级别低于17的设备上运行，则不会受到保护。 [Content Provider, targetSdkVersion >= 17]	警告	如果应用程序运行在一个API级别低于17的设备上，内容提供者(Content Provider)就会被导出。在这种情况下，它会被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。
4	Content Provider (androidx.core.content.FileProvider) 如果应用程序在API级别低于17的设备上运行，则不会受到保护。 [Content Provider, targetSdkVersion >= 17]	警告	如果应用程序运行在一个API级别低于17的设备上，内容提供者(Content Provider)就会被导出。在这种情况下，它会被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。
5	Broadcast Receiver (com.QBEIFZyG.HLsGcRHq.iWGglieEBChxVoty) 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。
6	Content Provider (com.QBEIFZyG.HLsGcRHq.dOZNhUrfnRlKqBui) 如果应用程序在API级别低于17的设备上运行，则不会受到保护。 [Content Provider, targetSdkVersion >= 17]	警告	如果应用程序运行在一个API级别低于17的设备上，内容提供者(Content Provider)就会被导出。在这种情况下，它会被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。
7	Content Provider (androidx.startup.InitializationProvider) 如果应用程序在API级别低于17的设备上运行，则不会受到保护。 [Content Provider, targetSdkVersion >= 17]	警告	如果应用程序运行在一个API级别低于17的设备上，内容提供者(Content Provider)就会被导出。在这种情况下，它会被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **0** | 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	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	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	13/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.PACKAGE_USAGE_STATS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	9/46	android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_NETWORK_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
www.xiaohongshu.com	安全	是	**IP地址:** 81.69.116.87 **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
• https://www.xiaohongshu.com/login/otherquestion	te2/n.java

• www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart	pr2/z.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	pr2/j.java
• https://www.xiaohongshu.com/experience/home?fullscreen=true	pr2/h.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	tr2/k.java
• https://www.xiaohongshu.com/experience/home?fullscreen=true	tr2/i.java
• www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart	tr2/a0.java
• https://www.xiaohongshu.com/login/otherquestion • www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart • https://www.xiaohongshu.com/experience/home?fullscreen=true • https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	自研引擎-S

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.appinstall.APP_KEY" : "vkq8br"

免责声明及风险提示: