MoGua

丰城专运 1.51.0.APK 分析报告

丰城专运 司机版

APP名称: 丰城专运

包名:	com.sf.freight.fczy
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年6月23日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: fczy-release-1.51.0_57_20220217.apk
文件大小: 40.62MB
MD5值: 67ca43a318f1e052786ff9b7e3e85f9b
SHA1值: b9de8c1f7f7c543b9dcdd0b500add200e6c62fdc
SHA256值: b0ebd46b2eab9db94720ad71b2e6575a5914c5cccc4f06c720760f85b02dc434

APP 信息

App名称: 丰城专运
包名: com.sf.freight.fczy
主活动Activity: com.sf.freight.fczy.main.SplashActivity
安卓版本名称: 1.51.0
安卓版本: 57

域名线索

URL线索

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=86, ST=guangdong, L=shenzhen, O=sf-express.com, OU=sf-express.com, CN=sf

签名算法: rsassa_pkcs1v15
有效期自: 2020-02-20 02:15:22+00:00
有效期至: 2060-02-10 02:15:22+00:00
发行人: C=86, ST=guangdong, L=shenzhen, O=sf-express.com, OU=sf-express.com, CN=sf
序列号: 0x7acefcf9
哈希算法: sha256
md5值: cb26aeafbe37dd15146e8e42994af1a9
sha1值: 70743ee02d5ddfa291e2640bfc4cf5d326199970
sha256值: db4ec7b2ef9e63e2f98e5c8661dab01ec2db0b536c2f807491ca55093fc91de8
sha512值: ae00165cf4eaf9685db39f8bcd771ab1c2c8dcfbbca213716e1d3d359cd9f067bf1aa1ef78025a6eb00eb73947566073bf20bf3fecdfe818569577c1739063c6
公钥算法: rsa
密钥长度: 2048
指纹: 53312f20538e2a6fa01385cf9f9fab5adde3d2b01ab539cd9fdf7b6e610ce5c8

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
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定数据。恶意应用可能会损坏你的系统的配置。

android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
com.sf.freight.fczy.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
		装载和卸载文	

android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.WRITE_INTERNAL_STORAGE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.sf.freight.fczy.main.SplashActivity	Schemes: fczy-app://, Hosts: sf-express.com, Paths: /action,