MoGua

韵达快递 8.5.7.APK 分析报告

APP名称:	韵达快递

包名:	com.yunda.app
域名线索:	2条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年9月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ydkd_21694.apk
文件大小: 68.43MB
MD5值: d5ab9a1457e8e5a3716fdbc1a513bcfa
SHA1值: 0d8f25603a7077916bfe7f20ba7ff2391a1f97d1
SHA256值: f3a346c553bf5dbe77e150dcbbf2a0bee4f68bdfe4a1e70ebc2a06bc0bac5735

APP 信息

App名称: 韵达快递
包名: com.yunda.app
主活动Activity: com.yunda.app.ui.SplashActivity
安卓版本名称: 8.5.7
安卓版本: 8050070

域名线索

域名	服务器信息
journeyapps.com	**IP**: 18.65.168.3 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

URL线索

URL信息	Url所在文件
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎

邮箱线索

手机线索

手机号	所在文件
18611111111	摸瓜V1引擎
13611111111	摸瓜V1引擎

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=86, ST=Shanghai, L=Shanghai, O=Yunda, OU=Yunda, CN=Yunda
签名算法: rsassa_pkcs1v15
有效期自: 2022-08-03 08:55:25+00:00
有效期至: 2121-07-10 08:55:25+00:00
发行人: C=86, ST=Shanghai, L=Shanghai, O=Yunda, OU=Yunda, CN=Yunda
序列号: 0x64dd93cd
哈希算法: sha256

md5值: 56c33895fc88b6bfb68015f3010f05d6
sha1值: c275a0333b9b331573f82aafe8cbeae1d35d7164
sha256值: 5dddbcb411a7dd912876ae5d8fe9d8c47e01590393e172b91858c5bcd3db77e7
sha512值: 710ab8928145163671ff8cc68b6d883fff281827fa3ed333e541f944c9e36be2134d8c8316985c198a5aa84e60a09429409ac93eebe52d5c528eb686e804b226
公钥算法: rsa
密钥长度: 2048
指纹: c2996d543c3af300cafc2a678d797aa57d32fe8ba7782ae3bcedcc003d30cfb3

🔑 硬编码敏感信息

可能的敏感信息
"bm_pwd_need" : "请输入电子面单联调密码"
"cancel_auth" : "取消授权"
"go_user" : "去使用"
"jiguang_privates_channel_high" : "HIGH"
"jiguang_privates_channel_low" : "LOW"
"jiguang_privates_channel_normal" : "NORMAL"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"not_auth" : "未认证"
"password" : "密码"
"pls_auth" : "请认证"

"real_name_authentic" : "实名认证"
"yunda_private" : "《韵达快递隐私政策》"
"jiguang_privates_channel_high" : "重要"
"jiguang_privates_channel_low" : "不重要"
"jiguang_privates_channel_normal" : "普通"

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**	**类型**	**详细情况**

	险		
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.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	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.ACCESS_COARSE_LOCATION	危	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

	险		用）。恶意应用程序可以使用它来确定您的大致位置
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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
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.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.RECORD_AUDIO	危	录音	允许应用程序访问音频记录路径

	险		
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
getui.permission.GetuiService.com.yunda.app	未知	Unknown permission	Unknown permission from android reference
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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.yunda.app.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.yunda.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.yunda.app.ui.MainActivity	Schemes: yunda://, Hosts: com.yunda.app, Ports: 8080, Paths: /home, /home/unipay,
com.yunda.app.ui.send.SendExpressActivity	Schemes: yunda://, Hosts: com.yunda.app, Ports: 8080, Paths: /send,
com.tencent.tauth.AuthActivity	Schemes: tencent100424468://, tencent1104652912://,

---