



MoGua

小鹿优享 1.6.4.APK 分析报告



APP名称:

小鹿优享

包名:	uni.UNIE3D4C0B
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件名: base.apk
文件大小: 31.37MB
MD5值: 65281d66e45e9948f7d8674fa4a1e6f6
SHA1值: 68903c71c46351b043bf1c75747c926f2fc8805f
SHA256值: 1369ad464013220805b51a1d04f299ec4d3214ac06dc5bb524243df892d60750

i APP 信息

App名称: 小鹿优享
包名: uni.UNIE3D4C0B
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.6.4
安卓版本: 164

🔍 域名线索

域名	服务器信息
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
	IP: 221.204.15.54 所属国家: China 地区: Shanxi

m3w.cn	城市: Taiyuan 纬度: 37.869438 经度: 112.561508
ask.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

 URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java

https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

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: True
找到 1 个唯一证书
主题: C=CN, ST=, L=, O=Android, OU=Android, CN=51FaopDbi1me6vHFLJxGnijlTKutjN%2FIPbBsrEAFx62FAaxkt1Nbf%2FMRYPx9WQKdTitbjbiErmYaLfk63JU5mg%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-02 07:31:09+00:00
有效期至: 2125-02-06 07:31:09+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=51FaopDbi1me6vHFLJxGnijlTKutjN%2FIPbBsrEAFx62FAaxkt1Nbf%2FMRYPx9WQKdTitbjbiErmYaLfk63JU5mg%3D%3D

序列号: 0xff10027
哈希算法: sha256
md5值: 87ed25925b31c12b1acfad6dfaf04842
sha1值: c34a963b4d37910716be749adb0747197f28e3ba
sha256值: e8c68788a44dc48a698684c685aa4397de562aaec4855a174bcb16ff7772bd8d
sha512值: 43b6b434edab51a6cdb7bfc29669a1dfea0976f4d2fddf6d630f59c998fab5a847a180789c5885a06c149ec7027b5626ce4532efd8264ce7361744a966f90134
公钥算法: rsa
密钥长度: 2048
指纹: a683a854ada2c3f4d74162eae60cb6691a7b3438d03627beb8d5db018f483a2f

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

	是		
--	---	--	--

向手机申请的权限	否 危 险	类型	详细情况
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_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.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_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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_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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统 需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。