MoGua

GENESIS 1.0.2.APK 分析报告

APP名称: GENESIS

包名:	uni.UNI4CE9379
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Genesis.apk
文件大小: 29.1MB
MD5值: c6ada4d882e321708caae8b270d44071
SHA1值: 2c8331b1212c3c961c8a4e32c3a52a0ea5c27b0d
SHA256值: 1684c0d53a2d2f2767b7e7162988621d1f99def79c1436a48325611eda8353d9

APP 信息

App名称: GENESIS
包名: uni.UNI4CE9379
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.2
安卓版本: 102

域名线索

域名	服务器信息
m3w.cn	**IP**: 124.163.195.65 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
ns.adobe.com	没有服务器地理信息.
schemas.android.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

er.dcloud.io	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ask.dcloud.net.cn	**IP**: 101.72.227.61 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
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

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://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/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.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=ktq84IaFRCg1hplHA8Dd92QQ3bOM5HKz1NDjGhtH%2B%2Fh1bpnvXUy452jYYZjEM6ySOimFdjPKQLUdgMbCCk822g%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-17 07:41:08+00:00
有效期至: 2124-11-23 07:41:08+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=ktq84IaFRCg1hplHA8Dd92QQ3bOM5HKz1NDjGhtH%2B%2Fh1bpnvXUy452jYYZjEM6ySOimFdjPKQLUdgMbCCk822g%3D%3D
序列号: 0x7c2aa886
哈希算法: sha256
md5值: 36db8758c2fc562dd86bde1aa936cbd5
sha1值: f877668a00165d31ba4a7d4512f8616fcbc34e20
sha256值: 4bb05fbb4253dc01e49bb6e84be1f4357d1afca865b37a75b4463d043021e639
sha512值: f4a746461753342b76743f9af5022f6c5d8673c8282e3e1822b139176264d45269cae0177eb32bcc24f722e681f1bc971bf9d8e3986fef1f07b376e942d0ddfa
公钥算法: rsa
密钥长度: 2048
指纹: 6cbcc1c3eee26bd273020c81475f94447111711b86660439855a9c4b9975d9e5

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.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
		在应用程序	

com.huawei.android.launcher.permission.CHANGE_BADGE	正常	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.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
uni.UNI4CE9379.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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.CALL_PRIVILEGED	系统需要	直接拨打任何电话号码	允许应用程序拨打任何电话号码,包括紧急电话号码,而无需您的干预。恶意应用程序可能会向紧急服务发出不必要和非法的呼叫
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.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