MoGua

# 精彩绮美拉 2.1.APK 分析报告

APP名称: 精彩绮美拉

| | |
|---|---|
| 包名: | plus.H59ACB198 |
| 域名线索: | 6条 |
| URL线索: | 15条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年6月21日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: 精彩绮美拉.apk
**文件大小**: 4.57MB
**MD5值**: e8d9a0e8e29d22140cee42c5a2688063
**SHA1值**: 8d99d8a378aa751eb029c69ec87a5a51aecfbcd9
**SHA256值**: 31f7f114f09481de7ea93af2bc6e6e0188a77bbe44499b54dbf7e154bc365b07

# APP 信息

**App名称**: 精彩绮美拉
**包名**: plus.H59ACB198
**主活动Activity**: io.dcloud.PandoraEntry
**安卓版本名称**: 2.1
**安卓版本**: 201

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| ns.adobe.com | 没有服务器地理信息. |
| m3w.cn | **IP**: 211.93.212.235<br>**所属国家**: China<br>**地区**: Beijing<br>**城市**: Beijing<br>**纬度**: 39.907501<br>**经度**: 116.397102 |
| er.dcloud.net.cn | **IP**: 43.142.57.168<br>**所属国家**: China<br>**地区**: Beijing<br>**城市**: Beijing<br>**纬度**: 39.907501<br>**经度**: 116.397102 |

| | |
|---|---|
| er.dcloud.io | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| ask.dcloud.net.cn | **IP**: 116.136.188.184<br>**所属国家**: China<br>**地区**: Nei Mongol<br>**城市**: Hohhot<br>**纬度**: 40.810650<br>**经度**: 111.650665 |

## URL线索

| URL信息 | Url所在文件 |
|---|---|
| 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://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |

| | |
|---|---|
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.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 |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |

# 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=o9N42cx2wX0tmF5UP3QC8ojD5cLJosYoGGG5o%2FseY9EfEIrjlUgbpJA2USFANoVAREBnoNZfLHTwlzjsHmhxNg%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-28 04:55:10+00:00
有效期至: 2124-06-04 04:55:10+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=o9N42cx2wX0tmF5UP3QC8ojD5cLJosYoGGG5o%2FseY9EfEIrjlUgbpJA2USFANoVAREBnoNZfLHTwlzjsHmhxNg%3D%3D
序列号: 0x17fb1a5
哈希算法: sha256
md5值: 49548267aed3c61dbb31f02454f0b0ff

sha1值: de063a033a9e65ef3f2c8b816e1c4e26c05e27d5
sha256值: 8a28cd2288e35fa7e73e39c6d3a6697d08ca0dd35997bdad4cf8165509d52bf8
sha512值: b9cc4825731445b629067a170608463326c1b127b8befd021c18711915648c6c98133960097fd8fb208c1f669e9b7baf74747d6f5d2b303a446e520084c2778b
公钥算法: rsa
密钥长度: 2048
指纹: bbb1b41a12f2abeb3554eee0cc2cad7584de0cb566ebfaff8092fd1f4e750ae6

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "dcloud_common_user_refuse_api" : "the user denies access to the API" |
| "dcloud_io_without_authorization" : "not authorized" |
| "dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service" |
| "dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed" |
| "dcloud_oauth_logout_tips" : "not logged in or logged out" |
| "dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained" |
| "dcloud_oauth_token_failed" : "failed to get token" |
| "dcloud_permissions_reauthorization" : "reauthorize" |
| "dcloud_tips_certificate" : "certificate" |
| "dcloud_common_user_refuse_api" : "用户拒绝该API访问" |
| "dcloud_io_without_authorization" : "没有获得授权" |
| "dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败" |

| |
|---|
| "dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败" |
| "dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败" |
| "dcloud_oauth_logout_tips" : "未登录或登录已注销" |
| "dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权" |
| "dcloud_oauth_token_failed" : "获取token失败" |
| "dcloud_permissions_reauthorization" : "重新授权" |
| "dcloud_tips_certificate" : "证书" |

## 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.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.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.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.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.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_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.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.WRITE_CONTACTS | 危险 | 写入联系人数 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来 |

| | | | |
|---|---|---|---|
| | | 据 | 删除或修改您的联系人数据 |
| 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.RECORD_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.READ_MEDIA_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ_MEDIA_VIDEO | 未知 | Unknown | Unknown permission from android reference |

| | | | |
|---|---|---|---|
| | | permission | |
| android.permission.READ_MEDIA_VISUAL_USER_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

# 应用内通信

| **活动**(ACTIVITY) | **通信**(INTENT) |
|---|---|
| io.dcloud.PandoraEntry | Schemes: h59acb198://, |