MoGua

中国新征程 3.5.7.APK 分析报告

APP名称:	中国新征程

包名:	uni.incbly
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17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 新征程[1].apk

文件大小: 25.74MB
MD5值: 7d437f1caa2dbc9cad660ee5d77929cb
SHA1值: 0836671c3f00d5384f35704b8206cd3e5001631b
SHA256值: 00daa5649ca76b964e8c994f384f7ba680c919b58f17fc4c67ddb33337435494

APP 信息

App名称: 中国新征程
包名: uni.incbly
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 3.5.7
安卓版本: 357

域名线索

域名	服务器信息
m3w.cn	**IP**: 221.204.15.111 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
er.dcloud.net.cn	**IP**: 43.142.57.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **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: 101.72.254.86 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
ns.adobe.com	没有服务器地理信息.

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

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=04J5g, ST=c8jhB, L=eJhw9, O=hr1745199474923, OU=jg1745199474923, CN=olct

签名算法: rsassa_pkcs1v15
有效期自: 2025-04-21 01:37:56+00:00
有效期至: 2075-04-09 01:37:56+00:00
发行人: C=04J5g, ST=c8jhB, L=eJhw9, O=hr1745199474923, OU=jg1745199474923, CN=olct
序列号: 0x17f90fc9
哈希算法: sha512
md5值: 5dd2ebdd7554e4dbbe8c5653a73baa36
sha1值: fea3e31423b3665025707f06f78e7a73823d1619
sha256值: 73a4ef808cd403d4b7969d5a09899edf63f26f1f0727c80f2843c39e61c95645
sha512值: 6d15bc082e515bc683c0b8898756b6d5dd7147c5f2c5229c784c65a3f52262d736c5c0196ee45b789d15ebbb5979c9e819c87ecf6968ee8bda45fbbbddc7f409
公钥算法: rsa
密钥长度: 4096
指纹: 305219127461502f71c92cd9093fb138a5e9ef5ab75a41d19ea918e222ba8588

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
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.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.incbly.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.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

应用内通信