MoGua

CloudChat 1.0.0.APK 分析报告

APP名称: CloudChat

包名:	com.ye202506021603
域名线索:	3条
URL线索:	2条
邮箱线索:	1条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.ye202506021603.apk
文件大小: 6.75MB
MD5值: bfec5ad45fdb0099713ca13b4995968d
SHA1值: 0f27eb7742d34c11959f00cbb693bc2cedcf9881
SHA256值: 2078a3c2127e7cc431bf9d0954c0089c67c0db865fad19d39e0f3ba76c095a57

APP 信息

App名称: CloudChat
包名: com.ye202506021603
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 10

域名线索

域名	服务器信息
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
dev.dcloud.net.cn	**IP**: 123.12.235.54 **所属国家**: China **地区**: Henan **城市**: Hebi **纬度**: 35.899170 **经度**: 114.192497
perfectionkills.com	**IP**: 192.30.252.153 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
http://dev.dcloud.net.cn/mui)	摸瓜V2引擎
http://ask.dcloud.net.cn/article/113';	摸瓜V2引擎
http://perfectionkills.com/global-eval-what-are-the-options/	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
houfeng@dcloud.io	摸瓜V2引擎

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=China, ST=ZheJiang, L=HangZhou, O=alias_75d1737e, OU=alias_75d1737e, CN=alias_75d1737e
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-02 08:03:01+00:00
有效期至: 2030-05-16 08:03:01+00:00
发行人: C=China, ST=ZheJiang, L=HangZhou, O=alias_75d1737e, OU=alias_75d1737e, CN=alias_75d1737e
序列号: 0x6d70ae79
哈希算法: sha256
md5值: 0d279b9839bd40ae35057e9387ab9da5
sha1值: 39ff39b7f5a9b73d7aa260dad0006265afcb412d
sha256值: d88b01b93c294d68893c386dffefc84e847e41f7356ee745dcee88fb0e2531ff
sha512值: db89c6460eca41db3f57f828dcc7e90f7cf567a6e9ce0c6f1b64aa69da7bc8d777c304fc367a53b6d2430a19b8bb270edecdf1ba81875d09cda6522f2b8244cd
公钥算法: rsa
密钥长度: 1024
指纹: 081345f811ae40a1b0139466fcc5b9acf1de2dd22519f6876c1759fa0dbe8e76

🔑 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_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.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_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

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
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.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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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.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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: h5b803654://,
