MoGua

在线服务 1.1.0.APK 分析报告

APP名称: 在线服务

包名:	uni.qvzaajatn.iknr
域名线索:	25条
URL线索:	27条
邮箱线索:	0条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 在线服务.apk
文件大小: 53.33MB
MD5值: 863cda0a886fce4f7d7e3f6f870a52da
SHA1值: 794291f20fd09015a172666e10711b7c744597d7
SHA256值: 770efd89755f21c064bae082732c26b74809732128eb6254e7fc05b6bdcad81a

APP 信息

App名称: 在线服务
包名: uni.qvzaajatn.iknr
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.0
安卓版本: 1

域名线索

域名	服务器信息
maps.googleapis.com	**IP**: 142.250.69.170 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.google.com	**IP**: 31.13.73.9 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
154.44.30.230	**IP**: 154.44.30.230 **所属国家**: United States of America **地区**: District of Columbia

	城市: Washington **纬度**: 38.901566 **经度**: -77.050781
vuejs.org	IP: 15.197.167.90 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
api.map.baidu.com	IP: 111.206.208.72 **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.
27.25.158.155	IP: 27.25.158.155 **所属国家**: China **地区**: Hubei **城市**: Shiyan **纬度**: 32.566669 **经度**: 110.783333
quilljs.com	IP: 172.66.40.163 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ns.adobe.com	没有服务器地理信息.
opensource.org	IP: 172.67.26.198 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ask.dcloud.net.cn	IP: 124.163.195.89 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
apis.map.qq.com	IP: 116.130.223.114 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
service.dcloud.net.cn	IP: 110.40.169.99 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

nrtc.netease.im	**IP**: 220.197.34.71 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
m3w.cn	**IP**: 221.204.15.87 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
117.50.201.232	**IP**: 117.50.201.232 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
111.170.19.85	**IP**: 111.170.19.85 **所属国家**: China **地区**: Hubei **城市**: Xiangyang **纬度**: 32.042267 **经度**: 112.144836
webtest.netease.im	**IP**: 111.124.202.79 **所属国家**: China **地区**: Guizhou **城市**: Zunyi **纬度**: 27.686441 **经度**: 106.907135
webapi.amap.com	**IP**: 222.138.194.17 **所属国家**: China **地区**: Henan **城市**: Luoyang **纬度**: 34.683289

	经度: 112.453911
map.qq.com	**IP**: 116.130.224.19 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.android.com	没有服务器地理信息.
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
180.97.221.102	**IP**: 180.97.221.102 **所属国家**: China **地区**: Jiangsu **城市**: Suzhou **纬度**: 31.311365 **经度**: 120.617691

URL线索

URL**信息**	Url**所在文件**
http://webtest.netease.im/nrtcproxy/nrtc/getSdkConfig.action	com/netease/lava/nertc/foreground/Authenticate.java
https://nrtc.netease.im/nrtc/getSdkConfig.action	com/netease/lava/nertc/foreground/Authenticate.java
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://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/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
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
http://117.50.201.232:9001	摸瓜V2引擎

http://180.97.221.102:9001	摸瓜V2引擎
http://111.170.19.85:9001	摸瓜V2引擎
http://154.44.30.230:9001	摸瓜V2引擎
http://27.25.158.155:9001	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://map.qq.com/api/js?v=2.exp&	摸瓜V2引擎
https://maps.googleapis.com/maps/api/js?	摸瓜V2引擎
https://webapi.amap.com/maps?v=2.0&	摸瓜V2引擎
https://api.map.baidu.com/api?type=webgl&v=1.0&	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎

http://117.50.201.232:9001	摸瓜V2引擎
http://180.97.221.102:9001	摸瓜V2引擎
http://111.170.19.85:9001	摸瓜V2引擎
http://154.44.30.230:9001	摸瓜V2引擎
http://27.25.158.155:9001	摸瓜V2引擎
https://github.com/Tencent/vConsole)	摸瓜V2引擎
http://opensource.org/licenses/MIT	摸瓜V2引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=WdGhd, ST=TbbHY, L=48nKE, O=og1749044717993, OU=xi1749044717993, CN=mngq
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-04 13:45:18+00:00
有效期至: 2075-05-23 13:45:18+00:00
发行人: C=WdGhd, ST=TbbHY, L=48nKE, O=og1749044717993, OU=xi1749044717993, CN=mngq
序列号: 0x4260f9d7
哈希算法: sha512
md5值: 544e0c436fff52c4f0c324a499f06439

sha1值: 458c2a9fe272faeb8feb63ae2fa519ecead52e17
sha256值: 10a68e9d35182969f3b915da56953c916daedec6cd025698f28f08341f19072d
sha512值: 55bc8094a4ce4b7e00968c9bc48fb105553f0285028091ec9a82efeaa2e2c7461da99dd77a1aa929e2663bf6d4cc53edab2b0a68ef67db3246ef33a18a348e24
公钥算法: rsa
密钥长度: 4096
指纹: 2f79d9004ffce8473c49c7767e79bdaf9d1811138cc724d8ea1e5b210b771352

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
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。
	未	Unknown	

com.vivo.notification.permission.BADGE_ICON	知	permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.POST_NOTIFICATIONS	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.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.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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备

android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.BIND_VOICE_INTERACTION	合法		VoiceInteractionService 必须要求,以确保只有系统可以绑定到它
android.permission.CAPTURE_AUDIO_OUTPUT	系统需要		允许应用程序捕获音频输出。
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	正常		允许应用程序捕获安全视频输出
android.permission.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
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_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

android.permission.CLEAR_APP_CACHE	系统需要	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。
android.permission.FACTORY_TEST	合法	在工厂测试模式下运行	作为低级制造商测试运行,允许完全访问手机硬件。仅当手机在制造商测试模式下运行时可用
android.permission.FORCE_BACK	合法	强制申请关闭	允许应用程序强制关闭前台的任何活动并返回。普通应用程序永远不需要
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.ANSWER_PHONE_CALLS	危险		允许应用接听来电。
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.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话

android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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

应用内通信