



MoGua

智慧建管 1.0.5.APK 分析报告



APP名称:

智慧建管

包名:	uni.UNIA325833
域名线索:	31条
URL线索:	22条
邮箱线索:	1条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件名: 智慧建管app.apk

文件大小: 18.86MB

MD5值: 426c1b5d948b677a40295348c3c1cac8

SHA1值: f358e3b76e832a35cc19f16e3484c747f695be25

SHA256值: fee02050b2a4c3d3a43b9641075bf2680bd8dac1c48ce8dff3ad56ba862820cf

i APP 信息

App名称: 智慧建管

包名: uni.UNIA325833

主活动Activity: io.dcloud.PandoraEntry

安卓版本名称: 1.0.5

安卓版本: 6

🔍 域名线索

域名	服务器信息
at.alicdn.com	IP: 60.222.200.243 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
api.next.bspapp.com	IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api.bspapp.com	IP: 39.96.249.142 所属国家: China 地区: Beijing

	<p>城市: Beijing 纬度: 39.907501 经度: 116.397102</p>
momentjs.com	<p>IP: 104.16.32.155 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>
lodash.com	<p>IP: 13.215.239.219 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281</p>
er.dcloud.io	<p>没有服务器地理信息.</p>
service.dcloud.net.cn	<p>IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102</p>
apis.map.qq.com	<p>IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102</p>
fontawesome.com	<p>IP: 104.18.23.52 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203</p>

npms.io	IP: 104.21.16.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cdn.nlark.com	IP: 101.72.238.91 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
image.weilanwl.com	没有服务器地理信息.
www.google.com	IP: 31.13.73.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
quilljs.com	IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
ns.adobe.com	没有服务器地理信息.

uniapp.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
192.168.67.47	IP: 192.168.67.47 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
m3w.cn	IP: 221.204.15.89 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
ossweb-img.qq.com	IP: 221.204.15.112 所属国家: China 地区: Shanxi 城市: Taiyuan

	纬度: 37.869438 经度: 112.561508
ask.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
img-cdn-qiniu.dcloud.net.cn	IP: 116.196.150.251 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
192.168.78.17	IP: 192.168.78.17 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
underscorejs.org	IP: 104.21.25.112 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
openjsf.org	IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut 纬度: 34.015400 经度: -117.858223
schemas.android.com	没有服务器地理信息.

fontawesome.comrn	没有服务器地理信息.
218.58.210.90	IP: 218.58.210.90 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
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

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://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://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/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
">https://lodash.com/>	摸瓜V2引擎
">https://openjsf.org/>	摸瓜V2引擎
">https://lodash.com/license>	摸瓜V2引擎
">http://underscorejs.org/LICENSE>	摸瓜V2引擎
https://npms.io/search?q=ponyfill	摸瓜V2引擎
http://192.168.67.47:8080/xps-vue/app	摸瓜V2引擎
https://image.weilanwl.com/color2.0/plugin/sylb2244.jpg	摸瓜V2引擎
https://image.weilanwl.com/color2.0/plugin/wdh2236.jpg	摸瓜V2引擎
https://image.weilanwl.com/color2.0/plugin/qpct2148.jpg	摸瓜V2引擎

https://image.weilanwl.com/color2.0/plugin/qpczd2307.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big3900	摸瓜V2引擎
http://192.168.67.47:8080/xps-vue	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big2100	摸瓜V2引擎
https://image.weilanwl.com/color2.0/plugin/cjkz2329.jpg	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/grid-2.png	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/grid-8.png	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/gird-3.png	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/grid-1.png	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/grid-7.png	摸瓜V2引擎
https://img-cdn-qiniu.dcloud.net.cn/uni-ui/grid-5.png	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big84000.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big37006.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big39000.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10001.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big25011.jpg	摸瓜V2引擎

https://ossweb-img.qq.com/images/lol/web201310/skin/big21016.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big99008.jpg	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
http://momentjs.com/guides/	摸瓜V2引擎
https://api.next.bspapp.com	摸瓜V2引擎
https://api.bspapp.com	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/secure-network.html	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise	摸瓜V2引擎
http://218.58.210.90:8800/xps-vue	摸瓜V2引擎
http://feross.org >	摸瓜V2引擎
http://192.168.78.17:3000	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big81005.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big25002.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big91012.jpg	摸瓜V2引擎
https://fontawesome.com \r\n	摸瓜V2引擎
https://fontawesome.com/license/free	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big91012.jpg)	摸瓜V2引擎

https://ossweb-img.qq.com/images/lol/web201310/skin/big10001.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/img/champion/Taric.png	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/img/champion/Morgana.png	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big81007.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big81020.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big81005.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big25002.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big91012.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big11010.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big114004.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big91005.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big99008.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10006.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10006.jpg	摸瓜V2引擎
https://image.weilanwl.com/gif/wave.gif	摸瓜V2引擎
https://image.weilanwl.com/gif/loading-black.gif	摸瓜V2引擎
https://image.weilanwl.com/gif/loading-white.gif	摸瓜V2引擎

https://image.weilanwl.com/gif/rhomb-black.gif	摸瓜V2引擎
https://image.weilanwl.com/gif/rhomb-white.gif	摸瓜V2引擎
https://image.weilanwl.com/gif/loading-1.gif	摸瓜V2引擎
https://image.weilanwl.com/gif/loading-2.gif	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10006.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10007.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big10001.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big107000.jpg	摸瓜V2引擎
https://ossweb-img.qq.com/images/lol/web201310/skin/big143004.jpg	摸瓜V2引擎
https://cdn.nlark.com/yuque/0/2019/png/280374/1552996358352-assets/web-upload/cc3b1807-c684-4b83-8f80-80e5b8a6b975.png);background-size:cover;background-position:50%;position:relative;z-index:1	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	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

邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com moment@2.30	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=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug

签名算法: rsassa_pkcs1v15

有效期自: 2021-04-12 08:27:53+00:00

有效期至: 2121-03-19 08:27:53+00:00

发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug

序列号: 0x363bc393

哈希算法: sha256

md5值: 06838cc840093b9d4689fc419ba1a3f3

sha1值: 97c84101b9141c130dd75d7428a2922518c36dcd

sha256值: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7

sha512值: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf

公钥算法: rsa

密钥长度: 2048

指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509

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_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	允许应用程序写入外部存储

		容	
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.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.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.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.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.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.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_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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。
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
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

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。