



# MoGua

## 和共物流 1.0.0.APK 分析报告



UNL LOGISTICS

APP名称:

和共物流

包名:	com.topode.dlms.site
域名线索:	9条
URL线索:	8条
邮箱线索:	2条
分析日期:	2024年10月19日
分析平台:	<a href="#">摸瓜APK反编译平台</a>

文件名: dlms\_site\_1.0.0.apk

文件大小: 27.62MB

MD5值: 168ec2cf80dfb508459741b7ef36bfbd

SHA1值: 45e63f0877af091d5c5010a1b583910a0ff37121

SHA256值: 21e56277c7cd233e63d047904f6dcde03a42de1b7a57a8b5f942b3d62e1ab4fd

## i APP 信息

App名称: 和共物流

包名: com.topode.dlms.site

主活动Activity: com.topode.dlms\_site.MainActivity

安卓版本名称: 1.0.0

安卓版本: 1

## 🔍 域名线索

域名	服务器信息
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
journeyapps.com	IP: 143.204.126.99 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
utms-api.urland.cn	IP: 120.79.134.19 所属国家: China 地区: Zhejiang

	<b>城市:</b> Hangzhou <b>纬度:</b> 30.293650 <b>经度:</b> 120.161423
schemas.android.com	没有服务器地理信息.
www.jsdelivr.com	<b>IP:</b> 92.223.84.84 <b>所属国家:</b> Germany <b>地区:</b> Hessen <b>城市:</b> Gallus <b>纬度:</b> 50.100380 <b>经度:</b> 8.629500
www.w3.org	<b>IP:</b> 104.18.22.19 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> San Francisco <b>纬度:</b> 37.775700 <b>经度:</b> -122.395203
developer.android.com	<b>IP:</b> 172.217.163.46 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> Mountain View <b>纬度:</b> 37.405991 <b>经度:</b> -122.078514
github.com	<b>IP:</b> 20.205.243.166 <b>所属国家:</b> United States of America <b>地区:</b> Washington <b>城市:</b> Redmond <b>纬度:</b> 47.682899 <b>经度:</b> -122.120903
flutter.dev	<b>IP:</b> 199.36.158.100 <b>所属国家:</b> United States of America <b>地区:</b> California <b>城市:</b> Mountain View <b>纬度:</b> 37.405991 <b>经度:</b> -122.078514

## URL线索

URL信息	Url所在文件
<a href="https://developer.android.com/guide/topics/permissions/overview">https://developer.android.com/guide/topics/permissions/overview</a>	io/flutter/plugin/platform/b.java
<a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>	x/i.java
<a href="https://journeyapps.com/">https://journeyapps.com/</a>	Mogua Engine V1
<a href="https://github.com/journeyapps/zxing-android-embedded">https://github.com/journeyapps/zxing-android-embedded</a>	Mogua Engine V1
<a href="https://www.jsdelivr.com/using-sri-with-dynamic-files">https://www.jsdelivr.com/using-sri-with-dynamic-files</a>	Mogua Engine V2
<a href="https://github.com/apvarun/toastify-js">https://github.com/apvarun/toastify-js</a>	Mogua Engine V2
<a href="http://www.w3.org/XML/1998/namespace">http://www.w3.org/XML/1998/namespace</a>	lib/arm64-v8a/libflutter.so
<a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>	lib/arm64-v8a/libflutter.so
<a href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/</a>	lib/arm64-v8a/libflutter.so
<a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a>	lib/arm64-v8a/libflutter.so
<a href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/</a>	lib/x86_64/libflutter.so
<a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a>	lib/x86_64/libflutter.so
<a href="http://www.w3.org/XML/1998/namespace">http://www.w3.org/XML/1998/namespace</a>	lib/x86_64/libflutter.so
<a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>	lib/x86_64/libflutter.so

<a href="http://www.w3.org/XML/1998/namespace">http://www.w3.org/XML/1998/namespace</a>	lib/armeabi-v7a/libflutter.so
<a href="http://www.w3.org/2000/xmlns/">http://www.w3.org/2000/xmlns/</a>	lib/armeabi-v7a/libflutter.so
<a href="https://www.w3.org/Style/CSS/Test/Fonts/Ahem/">https://www.w3.org/Style/CSS/Test/Fonts/Ahem/</a>	lib/armeabi-v7a/libflutter.so
<a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a>	lib/armeabi-v7a/libflutter.so
<a href="https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html">https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html</a>	lib/armeabi-v7a/libapp.so
<a href="https://utms-api.urland.cn/app/logistics-api/v1">https://utms-api.urland.cn/app/logistics-api/v1</a>	lib/armeabi-v7a/libapp.so
<a href="https://api.flutter.dev/flutter/material/Scaffold/of.html">https://api.flutter.dev/flutter/material/Scaffold/of.html</a>	lib/armeabi-v7a/libapp.so
<a href="https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android">https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android</a>	lib/armeabi-v7a/libapp.so
<a href="https://github.com/flutter/flutter/issues/new">https://github.com/flutter/flutter/issues/new</a>	lib/armeabi-v7a/libapp.so

## 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so
_httparser@13463476.responsepa storationinformation@863124995.fromserial _double@0150898.fromintege ._future@4048458.immediate  _growablelist@0150898._literal _link@14069316.fromrawpat c_growablelist@0150898.withcapaci _growablelist@0150898._literal6	

\_receiveportimpl@1026248.fromrawrec  
-\_list@0150898.\_ofarray  
z\_timer@1026248.periodic  
m\_growablelist@0150898.\_literal2  
g\_bigintimpl@0150898.from  
\_list@0150898.empty  
lectiontoolbarbutton@581113492.text  
c\_routedata@1134504625.ofroute  
\_directory@14069316.fromrawpat  
\_casterror@0150898.\_create  
l\_invocationmirror@0150898.\_withtype  
\_colorfilter@16065589.mode  
\_colorfilter@16065589.srgbtoline  
i\_rawsocket@14069316.\_writepipe  
lectiontoolbarbutton@459392285.text  
\_growablelist@0150898.\_literal1  
4\_uri@0150898.file  
q\_imagefilter@16065589.blur  
\_growablelist@0150898.\_literal4  
bb\_growablelist@0150898.\_ofgrowabl  
x\_growablelist@0150898.of  
k\_colorfilter@16065589.lineartosr  
\_nativesocket@14069316.pipe  
\_cookie@13463476.fromsetcoo  
authenticationscheme@13463476.fromstring  
\_list@0150898.of  
n\_typeerror@0150898.\_create  
\_list@0150898.\_ofgrowabl  
\_list@0150898.\_ofefficie  
\_growablelist@0150898.\_ofarray  
\_growablelist@0150898.\_literal3  
u\_growablelist@0150898.\_ofother  
\_timer@1026248.\_internal  
\_growablelist@0150898.\_literal5  
\_rawsocket@14069316.\_readpipe  
\_socket@14069316.\_readpipe  
\_list@0150898.\_ofother  
eo\_bytebuffer@7027147.\_new  
  
ngstreamssubscription@4048458.zoned  
\_assertionerror@0150898.\_create  
av\_nativesocket@14069316.normal  
j\_filestream@14069316.forstdin

lib/armeabi-v7a/libapp.so

\_uri@0150898.directory  
qd\_growablelist@0150898.\_literal8  
v\_file@14069316.fromrawpat  
gh\_growablelist@0150898.generate  
\_uri@0150898.notsimple  
7u\_growablelist@0150898.\_literal7  
\_future@4048458.zonevalue  
\_\_growablelist@0150898.\_ofefficie  
\_future@4048458.immediatee

## 手机线索

## 签名证书

APK已签名

v1 签名: True

v2 签名: True

v3 签名: False

找到 1 个唯一证书

主题: name=dlms\_site

签名算法: rsassa\_pkcs1v15

有效期自: 2023-03-08 07:38:21+00:00

有效期至: 3022-03-08 07:38:21+00:00

发行人: name=dlms\_site

序列号: 0x64083b6d

哈希算法: sha256

md5值: a4b0d73a1c4f9f7b6788f03fd03f4607

sha1值: 56d91af46206f5ffc4c3380a097a94610f25ace0

sha256值: 9c12e791e3933cf507e80861b47dc8398dcb00fa8beb1c706fded3236fb6a107

sha512值: 481071f3afdb3c3035bcc83a5bae3795abc966ed2dc1dbc0d8db83842ff1ed822eac7b36b17ad2f014ec3f30bda940d3df5db8dfe9b0ebfd65d0d5c3c16c35c4

公钥算法: rsa

密钥长度: 2048

指纹: 2c1e8e68e30be3e473664c0775145e16779648f9adde7d9dc42448247148e5d5

## 硬编码敏感信息



## 可能的敏感信息

"library\_zxingandroidembedded\_author" : "JourneyApps"

"library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"

## 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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

## 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。