MoGua

汇多多 2.0.9.APK 分析报告

APP名称:	汇多多
包名:	com.xinqu10.s
域名线索:	46条
URL线索:	71条
邮箱线索:	6条
分析日期:	2023年3月23日
分析平台:	摸瓜反编译平台

文件信息

文件名: base.apk
文件大小: 40.79MB
MD5值: e9fff11f326b2b364a81992732b46871
SHA1值: 5ce4b30d338100bcc82f6406ac9a87dc17407fd7
SHA256值: ad45e21ac278f43e8120759fe61ed6ed6b21370e115e085ea9c91abed88d9e24

APP 信息

App名称: 汇多多
包名: com.xinqu10.s
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 2.0.9
安卓版本: 209

域名线索

域名	服务器信息
long.open.weixin.qq.com	**IP:** 109.244.217.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
api.weixin.qq.com	**IP:** 81.69.216.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
dualstack-a.apilocate.amap.com	**IP:** 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
daneden.github.io	**IP:** 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
wap.amap.com	**IP:** 42.81.21.238 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666

域名	服务器信息
service.dcloud.net.cn	IP: 121.40.221.59 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
opensource.org	IP: 172.67.197.41 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
dualstack-arestapi.amap.com	IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
maps.testing.amap.com	IP: 140.205.69.9 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

域名	服务器信息
at.alicdn.com	IP: 220.181.135.251 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
quilljs.com	IP: 216.24.57.3 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.openssl.org	IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

域名	服务器信息
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
apis.map.qq.com	IP: 109.244.244.223 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apilocate.amap.com	IP: 59.82.31.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mpsapi.amap.com	IP: 203.119.169.143 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
www.crmeb.com	IP: 47.97.2.242 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
clipboardjs.com	IP: 172.67.168.158 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
lbs.amap.com	IP: 59.82.31.203 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apis.xinqu10.com	IP: 39.108.144.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

域名	服务器信息
cgicol.amap.com	IP: 59.82.31.156 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apiinit.amap.com	IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
m3w.cn	IP: 36.102.212.110 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
yuntuapi.amap.com	没有服务器地理信息.
wprd0d.is.autonavi.com	没有服务器地理信息.
mos.m.taobao.com	IP: 124.238.245.244 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717

域名	服务器信息
crbug.com	**IP:** 216.239.32.29 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514
ask.dcloud.net.cn	**IP:** 36.102.212.106 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423
open.weixin.qq.com	**IP:** 175.24.209.30 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232
abroad.apilocate.amap.com	**IP:** 59.82.44.11 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423

域名	服务器信息
restsdk.amap.com	IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
adiu.amap.com	IP: 59.82.31.67 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
img1.imgtn.bdimg.com	IP: 218.68.136.48 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
m5.amap.com	IP: 106.11.35.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

域名	服务器信息
s.xinqu10.com	IP: 39.108.144.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
mps.amap.com	IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
ns.adobe.com	没有服务器地理信息.
lame.sf.net	IP: 104.18.26.198 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.google.com	IP: 104.244.43.167 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

域名	服务器信息
wb.amap.com	IP: 59.82.31.67 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
stream.mobihtml5.com	IP: 153.3.236.79 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779
stream.dcloud.net.cn	IP: 47.99.87.63 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
schemas.android.com	没有服务器地理信息.
mst01.is.autonavi.com	IP: 203.119.169.44 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

域名	服务器信息
192.168.0.70	**IP:** 192.168.0.70 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/access_token? appid=%s&secret=%s&code=%s&grant_type=authorization_code	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/refresh_token? appid=%s&grant_type=refresh_token&refresh_token=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
http://lbs.amap.com/api/android-sdk/guide/error/	io/dcloud/js/map/amap/adapter/AMapLink.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/e/c/h/b.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
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.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://restsdk.amap.com/v3	com/amap/api/col/p0003s/et.java
https://restsdk.amap.com/v3	com/amap/api/col/p0003s/et.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003s/et.java

URL信息	Url所在文件
https://restsdk.amap.com/v4	com/amap/api/col/p0003s/et.java
http://restsdk.amap.com/v5	com/amap/api/col/p0003s/et.java
https://restsdk.amap.com/v5	com/amap/api/col/p0003s/et.java
http://yuntuapi.amap.com	com/amap/api/col/p0003s/et.java
https://yuntuapi.amap.com	com/amap/api/col/p0003s/et.java
http://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003s/et.java
https://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/p0003s/et.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003s/et.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/p0003s/et.java
https://adiu.amap.com/ws/device/adius	com/amap/api/col/p0003s/ji.java
https://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003s/in.java
http://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003s/in.java
http://apilocate.amap.com/mobile/binary	com/amap/api/col/p0003s/lb.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/amap/api/col/p0003s/lb.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003s/i.java

URL信息	Url所在文件
http://restsdk.amap.com/v4/grasproad/driving?	com/amap/api/col/p0003s/gz.java
http://restsdk.amap.com	com/amap/api/col/p0003s/hp.java
http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003s/gt.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/col/p0003s/gt.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/col/p0003s/gt.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/col/p0003s/gt.java
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\	com/amap/api/col/p0003s/b.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/p0003s/hf.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/p0003s/hf.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/col/p0003s/cs.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003s/cs.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/p0003s/hg.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003s/ct.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003s/cf.java
http://wap.amap.com/	com/amap/api/maps/AMapUtils.java

URL信息	Url所在文件
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/fe.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/fe.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fo.java
http://restsdk.amap.com	com/loc/v.java
https://restsdk.amap.com/sdk/compliance/params	com/loc/ap.java
http://restsdk.amap.com/sdk/compliance/params	com/loc/ap.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/m.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/m.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
http://apilocate.amap.com/mobile/binary	com/loc/fj.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/fj.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fj.java

URL信息	Url所在文件
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cv.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fc.java
https://adiu.amap.com/ws/device/adius	com/loc/bf.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/autonavi/amap/mapcore/Inner_3dMap_location.java
http://m5.amap.com/	com/autonavi/base/amap/mapcore/maploader/AMapLoader.java
http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mst01.is.autonavi.com/appmaptile? z=%d&x=%d&y=%d&lang=zh_cn&size=1&scale=1&style=6	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mpsapi.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://daneden.github.io/animate.css/\n	Mogua Engine V2
http://opensource.org/licenses/MIT\n	Mogua Engine V2

URL信息	Url所在文件
https://at.alicdn.com/t/font_993865_9ndsg8a4fw6.woff2?t=1652340001187)	Mogua Engine V2
https://at.alicdn.com/t/font_993865_9ndsg8a4fw6.woff?t=1652340001187)	Mogua Engine V2
https://at.alicdn.com/t/font_993865_9ndsg8a4fw6.ttf?t=1652340001187)	Mogua Engine V2
https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://apis.map.qq.com/tools/geolocation?key=	Mogua Engine V2
https://apis.map.qq.com/uri/v1/geocoder?coord=	Mogua Engine V2
http://apis.xinqu10.com/spring/getExpressInfo?no=	Mogua Engine V2
http://apis.xinqu10.com/spring/getSpreadUid?invitationCode=	Mogua Engine V2

URL信息	Url所在文件
http://apis.xinqu10.com/spring/uid?uid=	Mogua Engine V2
http://apis.xinqu10.com/spring/addUserMerchant?uid=	Mogua Engine V2
http://apis.xinqu10.com/spring/spreadlist?merId=	Mogua Engine V2
http://192.168.0.70:9527/kefu/dashboard02?mer_id=3&uid=167&msn=\u7cfb\u7edf\u901a\u77e5\uff01\u589e\u52a0	Mogua Engine V2
http://apis.xinqu10.com/spring/frame_url?id=0	Mogua Engine V2
http://img1.imgtn.bdimg.com/it/u=451604666,2295832001&fm=26&gp=0.jpg	Mogua Engine V2
https://s.xinqu10.com	Mogua Engine V2
http://apis.xinqu10.com/spring/addStoreService?merId=	Mogua Engine V2
https://mos.m.taobao.com/itaobao/aitbh5?__bucket__=1&union_biz_trans=%7B%22shunt%22%3A%223973_2_1%22%7D	Mogua Engine V2
http://apis.xinqu10.com/spring/frame_url?id=	Mogua Engine V2
http://apis.xinqu10.com/spring/frame_url?id=1	Mogua Engine V2
http://apis.xinqu10.com	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
https://clipboardjs.com/	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2

URL信息	Url所在文件
https://quilljs.com	Mogua Engine V2
https://www.crmeb.com	Mogua Engine V2
https://www.crmeb.com	Mogua Engine V2
https://www.crmeb.com	Mogua Engine V2
https://www.crmeb.com	Mogua Engine V2
https://crbug.com/v8/8520	lib/x86/libweexjss.so
http://lame.sf.net	lib/x86/liblamemp3.so
http://www.openssl.org/support/faq.html	lib/x86/libijkffmpeg.so
http://mpsapi.amap.com/ws/mps/vmap	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/rtt	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/smap	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/	lib/x86/libAMapSDK_MAP_v9_2_0.so

URL信息	Url所在文件
http://m5.amap.com	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/rtt	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/vmap	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/smap	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/spot	lib/x86/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/hot	lib/x86/libAMapSDK_MAP_v9_2_0.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so
http://mpsapi.amap.com/ws/mps/vmap	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/rtt	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/smap	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so

URL信息	Url所在文件
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
http://mpsapi.amap.com/	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
http://m5.amap.com	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/rtt	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/vmap	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/smap	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/spot	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so
https://mps.amap.com/ws/mps/hot	lib/armeabi-v7a/libAMapSDK_MAP_v9_2_0.so

邮箱线索

邮箱地址	所在文件
admin@crmeb.com	Mogua Engine V2
admin@crmeb.com	Mogua Engine V2

邮箱地址	所在文件
admin@crmeb.com	Mogua Engine V2
admin@crmeb.com	Mogua Engine V2
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

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: False
找到 1 个唯一证书
主题: C=CN, ST=guangdong, L=Shenzhen, O=xqs, OU=xqs, CN=ljyczu
签名算法: rsassa_pkcs1v15
有效期自: 2022-10-14 11:08:58+00:00
有效期至: 2122-09-20 11:08:58+00:00
发行人: C=CN, ST=guangdong, L=Shenzhen, O=xqs, OU=xqs, CN=ljyczu
序列号: 0x694d1131300f86cc
哈希算法: sha256

md5值: 0c7816257ca3fb9bb840577955f94228
sha1值: 196f0dc0e163bd86cd4f5799df65466d801e4236
sha256值: 853ca7f4710406fcfbe823fa04f09db35816f32d1ff1a5ce13ef7ab2c7bbf481
sha512值: b8d3d87f69a57ee06764d1b735d96678e45fcf21828f3ffe9c45eaa2353f018c043e189b566662829a4209aaee87a7f3cf69f7a162f0c41acc351c7d176372c9
公钥算法: rsa
密钥长度: 2048
指纹: 40f7f6f93087e92b6c55881206de849aa1b02ea746c46672c1e4c2952fbdb67f

🔑 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_feature_oauth_weixin_plugin_description" : "wechat"
"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_common_user_refuse_api" : "用户拒绝该API访问"

可能的敏感信息
"dcloud_feature_oauth_weixin_plugin_description" : "微信"
"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"

加壳分析

第三方SDK

名称	分类	URL链接
fastjson	开发辅助	https://reports.exodus-privacy.eu.org/trackers/457
数字天堂（北京）网络技术有限公司	APP打包, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/444

名称	分类	URL链接
腾讯微信	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/447
高德地图	位置服务	https://reports.exodus-privacy.eu.org/trackers/361

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/删除外部存储内容	允许应用程序写入外部存储
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

向手机申请的权限	是否危险	类型	详细情况
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.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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。

向手机申请的权限	是否危险	类型	详细情况
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.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_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。这使它能够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.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.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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