MoGua

pos点餐 1.0.0.APK 分析报告

APP名称:	pos点餐

包名:	com.riest.zdgj.pos_canteen
域名线索:	24条
URL线索:	45条
邮箱线索:	0条
分析日期:	2025年7月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: __UNI__B0CEF51_20250605172715.apk
文件大小: 44.73MB
MD5值: a4bf64d2079808f36a1fe1c99315a505
SHA1值: d40d9cd734bbe4364ba4b3fb6f9c2580ac37f153
SHA256值: 4ff4ca5164da61d1fcab7a8cb455a121e636af749dda5829486c52081c0dc6f8

APP 信息

App名称: pos点餐
包名: com.riest.zdgj.pos_canteen
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 120

域名线索

域名	服务器信息
gtc.getui.nethttps	没有服务器地理信息.
b-gtc.getui.nethttps	没有服务器地理信息.
restsdk.amap.com	**IP**: 59.82.132.217 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
restapi.amap.com	**IP**: 59.82.132.217 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

dualstack-arestapi.amap.com	**IP**: 59.82.132.217 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
c-gtc.getui.nethttps	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
cgicol.amap.com	**IP**: 110.253.188.148 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
m3w.cn	**IP**: 221.204.20.165 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
dualstack-a.apilocate.amap.com	**IP**: 106.11.43.81 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

ns.adobe.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
nisportal.10010.com	**IP**: 124.64.196.20 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
lbs.amap.com	**IP**: 110.253.189.212 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
zxid-m.mobileservice.cn	**IP**: 101.69.207.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
aid.mobileservice.cn	**IP**: 101.69.207.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
adiu.amap.com	**IP**: 110.253.189.146 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349

er.dcloud.io	没有服务器地理信息.
apilocate.amap.com	**IP**: 106.11.43.81 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
c-hzgt2.getui.com	**IP**: 124.160.155.57 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000
abroad.apilocate.amap.com	**IP**: 59.82.44.11 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
sdk-open-phone.getui.com	**IP**: 101.68.218.177 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000
d-gt.getui.com	没有服务器地理信息.

URL线索

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
https://c-gtc.getui.net,https://c-gtc.gepush.com	com/getui/gtc/c/b.java
https://gtc.getui.net,https://gtc.gepush.com	com/getui/gtc/c/b.java
https://b-gtc.getui.net,https://b-gtc.gepush.com	com/getui/gtc/c/b.java
https://sdk-open-phone.getui.com/	com/getui/gtc/i/d/b.java
https://sdk-open-phone.getui.com/api.php	com/igexin/push/a.java
https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
https://bi.	com/igexin/push/config/b.java
https://config.	com/igexin/push/config/b.java
https://bi.	com/igexin/push/config/h.java
https://config.	com/igexin/push/config/h.java
https://adiu.amap.com/ws/device/adius	com/loc/bo.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/df.java
http://apilocate.amap.com/mobile/binary	com/loc/fv.java

http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/fv.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fv.java
https://restsdk.amap.com/sdk/compliance/params	com/loc/ay.java
http://restsdk.amap.com/sdk/compliance/params	com/loc/ay.java
http://restsdk.amap.com	com/loc/w.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
https://restapi.amap.com/rest/aaid/get	com/loc/ag.java
http://restapi.amap.com/rest/aaid/get	com/loc/ag.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/n.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/n.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/gb.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fo.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/fq.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/fq.java
https://aid.mobileservice.cn/	com/zx/a/l8b7/j3.java

https://nisportal.10010.com:9001	com/zx/a/I8b7/f1.java
https://zxid-m.mobileservice.cn/sdk/config/v2/init	com/zx/a/I8b7/n.java
https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/I8b7/l.java
https://zxid-m.mobileservice.cn/sdk/app/depAnalysis	com/zx/a/I8b7/d1.java
https://zxid-m.mobileservice.cn/sdk/module/getCoreModule	com/zx/a/I8b7/f0.java
https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken	com/zx/a/I8b7/v1.java
https://zxid-m.mobileservice.cn/sdk/extend/tag	com/zx/a/I8b7/b2.java
https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/I8b7/w1.java
https://zxid-m.mobileservice.cn/sdk/ext/pconfig	com/zx/a/I8b7/f.java
https://zxid-m.mobileservice.cn/sdk/channel/report	com/zx/a/I8b7/p1.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://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/35058	io/dcloud/feature/audio/AudioRecorderMgr.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

邮箱线索

手机线索

手机号	所在文件
14222222222	com/loc/n.java
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=, L=, O=Android, OU=Android, CN=ySRTLUCJDAovovmvgWFyTMQxjPqSRbpAbShaH8GwvwpIXwtQBYvGK%2FKlJjhkstN87sNQPzdzJIPXLKOIAlZYxQ%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-10 01:57:12+00:00
有效期至: 2124-12-17 01:57:12+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=ySRTLUCJDAovovmvgWFyTMQxjPqSRbpAbShaH8GwvwpIXwtQBYvGK%2FKlJjhkstN87sNQPzdzJIPXLKOIAlZYxQ%3D%3D
序列号: 0x1d8cf483
哈希算法: sha256
md5值: d78b6d44505bb1458f6282ca18583aab
sha1值: fcd10f2f15bf80b3945d666d438b2c45439abef1
sha256值: 4ead6ca806d6efe24e770c7e4c0a3f6a57d53f7f5c261cc5090173d10c43b856
sha512值: 84e49a0764f46b16a33ba7897f10502b37a7e65c40b4ac631e8767c4d511578fb214e74ba558280d9ddcc86938a9e7263cc8b04126b2c71f149b0d481fa67f6a
公钥算法: rsa
密钥长度: 2048
指纹: 7ac13d660ac7c04db5259c0f2c2604b17c0c60f7f81d7fed7c2849a7c3359a59

硬编码敏感信息

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**

登陆搜瓜网站后查看		

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。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
getui.permission.GetuiService.com.riest.zdgj.pos_canteen	未知	Unknown permission	Unknown permission from android reference
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
com.riest.zdgj.pos_canteen.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
android.permission.ACCESS_FINE_LOCATION	危	精细定位	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

	险	（GPS）	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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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.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.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_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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_SCAN	未知	Unknown permission	Unknown permission from android reference

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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: unipush://, Hosts: io.dcloud.unipush, Paths: /,

---