MoGua

铁塔换电运维 1.4.10.APK 分析报告

中国铁塔
运维版

APP名称: 铁塔换电运维

包名:	com.chinatower.towerEle4
域名线索:	6条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年5月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.chinatower.towerEle4_1.4.10_150.apk
文件大小: 73.15MB
MD5值: e9023697cc9a9ba3a2a2db49d7956c54
SHA1值: 8ac51052bafeb384e116a2e5abf411a0bac3070a
SHA256值: 5616c8062dc8e3e7ba52cc0ca9e6f0d4df3023b0d8eb2f1e69ccce832c13689c

APP 信息

App名称: 铁塔换电运维
包名: com.chinatower.towerEle4
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.4.10
安卓版本: 150

域名线索

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
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
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
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
ask.dcloud.net.cn	**IP**: 36.102.212.39 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
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

URL线索

URL**信息**	Url**所在文件**
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
http://mpsapi.amap.com/ws/mps/vmap/	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/rtt/	lib/armeabi/libAMapSDK_MAP_v9_5_0.so

http://mpsapi.amap.com/ws/mps/smap	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/rtt	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/vmap	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/smap	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/spot	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/hot	lib/armeabi/libAMapSDK_MAP_v9_5_0.so
https://crbug.com/v8/8520	lib/x86/libweexjss.so
https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so

邮箱线索

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: C=86, ST=ln, L=dl, O=jnsd, OU=jnsddl, CN=zwj
签名算法: rsassa_pkcs1v15
有效期自: 2020-10-19 09:34:46+00:00
有效期至: 2120-09-25 09:34:46+00:00
发行人: C=86, ST=ln, L=dl, O=jnsd, OU=jnsddl, CN=zwj
序列号: 0x30dfa430
哈希算法: sha256
md5值: 2cd748037085da50155e13260f5f79b4
sha1值: b773f1f6893cc302bae96e87e8906765a910c566
sha256值: 41cb5682ad9f838926ae284068c40306c48e99942542ce09b875d3e258a7ccfb
sha512值: 37297e6cfd60e09ba770b6ce1e92204963b2aabb55ff5e93c3744d27990b6188390b7fdfc737dddfb4366f0224d42cdd3e2d65b318f451c3a6438c46cdeb87c3
公钥算法: rsa
密钥长度: 2048
指纹: 558028c864239085f67e0d265912a8f231a7b1e0ceb669eb2904e9b17f59ed5d

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_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"

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.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.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.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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
		更改您的音频	

android.permission.MODIFY_AUDIO_SETTINGS	正常	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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.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.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.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。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	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。
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
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.chinatower.towerEle4.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.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.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.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.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

com.chinatower.towerEle4.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntryActivity	Schemes: h56131bcf://,
