



MoGua

GWM ORA 1.9.1.APK 分析报告



APP名称:

GWM ORA

包名:	com.ora.germany
域名线索:	5条
URL线索:	5条
邮箱线索:	1条
分析日期:	2025年4月28日
分析平台:	摸瓜APK反编译平台

文件名: GWM_ORA_1.9.1.apk
文件大小: 138.52MB
MD5值: 61d707e4ccbdf50a3fc3d49f5a63963f
SHA1值: 5586f0eeff3c32e4db636e6bcd38111c2d8071e
SHA256值: f5803c42e321a7ba0bc0467564f629b2ef50a825d61e475a5c17b84ed65199dd

i APP 信息

App名称: GWM ORA
包名: com.ora.germany
主活动Activity: com.gdc.ora.ui.SplashActivity
安卓版本名称: 1.9.1
安卓版本: 59

🔍 域名线索

域名	服务器信息
www.zetetic.net	IP: 13.225.165.105 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
1.aerial.maps.ls.hereapi.com	IP: 143.204.86.11 所属国家: Japan 地区: Tokyo

	城市: Tokyo 纬度: 35.689507 经度: 139.691696
traffic.vector.hereapi.com	IP: 52.220.240.215 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
vector.hereapi.com	IP: 143.204.126.100 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696

 URL线索

URL信息	Url所在文件
https://www.zetetic.net/sqlcipher/	Mogua Engine V1
https://www.zetetic.net/sqlcipher/license/	Mogua Engine V1
https://github.com/sqlcipher/android-database-sqlcipher	Mogua Engine V1
https://traffic.vector.hereapi.com/v2/traffictiles/flow/mc/	Mogua Engine V2
https://traffic.vector.hereapi.com/v2/traffictiles/incident/mc/	Mogua Engine V2
https://vector.hereapi.com/v2/vectortiles/base/mc/	Mogua Engine V2

✉

邮箱线索

邮箱地址	所在文件
dataprotection@gwm-eu.com	Mogua Engine V1

☰

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=86, ST=shanghai, L=shanghai, O=GWM, OU=GDC, CN=Great Wall Motor Co.Ltd
签名算法: rsassa_pkcs1v15
有效期自: 2020-10-21 02:40:42+00:00
有效期至: 3020-02-22 02:40:42+00:00
发行人: C=86, ST=shanghai, L=shanghai, O=GWM, OU=GDC, CN=Great Wall Motor Co.Ltd
序列号: 0x63e4a114
哈希算法: sha256
md5值: 63b9adbad081edbf0d6983397f3ded91
sha1值: 62a5665e5873921cb26a950f8ab1c490032d2da9
sha256值: 08c70ab68fce152ffed72d730af1597540496fe589b252c30420aaec4ba31583
sha512值: eee14a8522517d9d0162738277878b95aa214f9d10db1091d1b14d33dcd26b82b63ec094523b0cdfb07a4adc475451341b2a9a329b78783ba77173eddc19acb8
公钥算法: rsa
密钥长度: 2048
指纹: 9d62b8d5e3c61f473a378ecd3356069600a69a2d61ad08e2bbd8a8fe9fb3cc7a

硬编码敏感信息

可能的敏感信息
"ac_account_login_with_password" : "Login with password"
"ac_account_password" : "Password"
"ac_incorrect_email_or_password" : "Incorrect email or password"
"ac_modify_password" : "Change Password"
"ac_reset_password" : "Reset Password"
"ac_set_safe_password" : "Set PIN"
"ac_setup_password" : "Set Password"
"base_agree_authority" : "Don't allow"
"base_apply_authority" : ""%1\$s" needs access to your %2\$s"
"base_auth_later" : "Authorize later"
"base_auth_now" : "Authorize now"
"base_authority_type" : "%1\$s Authority"
"base_authorize" : "Authorize"
"base_engine_auth_success" : "Succeed"
"base engine grant auth" : "Car log in authority"

"base_engine_login_auth" : "Vehicle account login confirmation"
"base_forget_password" : "Forgot password?"
"base_mysterious_user" : "No Data"
"base_refuse_authority" : "OK"
"base_token_lose_tips" : "Token error"
"com.twitter.sdk.android.CONSUMER_KEY" : "XaB7ecDQaLYMpiDMAwqbqZ4XJ"
"com.twitter.sdk.android.CONSUMER_SECRET" : "MABhpzpaGy0N02xTgNICpDS6vAwYuuUqtCMYz681LYFVZ3VeHC"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"google_api_key" : "AlzaSyDpbVYZbTmiZQ_GGWowqrqC8rcPy0VdFsw"
"google_crash_reporting_api_key" : "AlzaSyDpbVYZbTmiZQ_GGWowqrqC8rcPy0VdFsw"
"library_android_database_sqlcipher_author" : "Zetetic, LLC"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"permission_apply_authority" : ""%1\$s" needs access to your %2\$s"
"permission_authority_type" : "%1\$s Authority"
"ve_auth_vehicle_account_login_tips" : "Do you want to authorize the vehicle account login?"
"ve_authorize" : "Authorize"
"ac_account_login_with_password" : "Mit Passwort anmelden"

"ac_account_password" : "Passwort"
"ac_incorrect_email_or_password" : "E-Mail-Adresse oder Passwort ungültig"
"ac_modify_password" : "Passwort ändern"
"ac_reset_password" : "Passwort zurücksetzen"
"ac_set_safe_password" : "PIN festlegen"
"ac_setup_password" : "Passwort erstellen"
"base_agree_authority" : "Nicht erlauben"
"base_apply_authority" : ", „%1\$s“ benötigt Zugriff auf dein %2\$s"
"base_auth_later" : "Später erlauben"
"base_auth_now" : "Jetzt erlauben"
"base_authority_type" : "%1\$s Berechtigung"
"base_authorize" : "Autorisieren"
"base_engine_auth_success" : "Erfolgreich"
"base_engine_grant_auth" : "Automobil-Login autorisieren"
"base_engine_login_auth" : "Anmeldebestätigung für das Fahrzeugkonto"
"base_forget_password" : "Passwort vergessen?"
"base_mysterious_user" : "Keine Daten"
"base_refuse_authority" : "OK"

"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"permission_apply_authority" : "„%1\$s“ benötigt Zugriff auf %2\$s"
"permission_authority_type" : "Zugriff auf %1\$s"
"ve_auth_vehicle_account_login_tips" : "Möchtest du die Anmeldung des Fahrzeugkontos autorisieren?"
"ac_account_login_with_password" : "התחברות באמצעות סיסמה"
"ac_account_password" : "סיסמה"
"ac_incorrect_email_or_password" : "דוא"ל או סיסמה שגויים"
"ac_modify_password" : "שינוי סיסמה"
"ac_reset_password" : "איפוס סיסמה"
"ac_set_safe_password" : "הגדרת קוד סודי"
"ac_setup_password" : "הגדרת סיסמה"
"base_agree_authority" : "אל תאפשר"
"base_apply_authority" : "שלך צריך הרשאת גישה ל-%2\$s ""%1\$s""
"base_auth_later" : "אחר כך"
"base_auth_now" : "מתן הרשאות"
"base_authority_type" : "הרשאה %1\$s"
"base_authorize" : "אישור"

"base_engine_auth_success" : "ההרשאה הצליחה"
"base_engine_grant_auth" : "הרשאת התחברות לרכב"
"base_engine_login_auth" : "אשר התחברות רכב"
"base_forget_password" : "שכחת סיסמה?"
"base_mysterious_user" : "המשתמש הזה מאוד מסתורי"
"base_refuse_authority" : "אישור"
"permission_apply_authority" : ""%1\$s" %2\$s לגישה ל-זקוק שלך"
"permission_authority_type" : "%1\$s של סמכות"
"ve_auth_vehicle_account_login_tips" : "האם ברצונך לאשר את ההתחברות לחשבון הרכב?"
"ac_account_login_with_password" : "Login with password"
"ac_account_password" : "Password"
"ac_incorrect_email_or_password" : "Incorrect email or password"
"ac_modify_password" : "Change Password"
"ac_reset_password" : "Reset Password"
"ac_set_safe_password" : "Set PIN"
"ac_setup_password" : "Set Password"
"base_agree_authority" : "Don't allow"
"base_apply_authority" : ""%1\$s" needs access to your %2\$s"

"base_auth_later" : "Authorize later"
"base_auth_now" : "Authorize now"
"base_authority_type" : "%1\$s Authority"
"base_authorize" : "Authorize"
"base_engine_auth_success" : "Succeed"
"base_engine_grant_auth" : "Car Login Authority"
"base_engine_login_auth" : "Vehicle account login confirmation"
"base_forget_password" : "Forgot password?"
"base_mysterious_user" : "No Data"
"base_refuse_authority" : "OK"
"base_token_lose_tips" : "Token error"
"permission_apply_authority" : ""%1\$s" needs access to your %2\$s"
"permission_authority_type" : "%1\$s Authority"
"ve_auth_vehicle_account_login_tips" : "Do you want to authorize the vehicle account login?"
"ve_authorize" : "Authorize"
"ac_account_login_with_password" : "Logga in med lösenord"
"ac_account_password" : "Lösenord"

"ac_incorrect_email_or_password" : "Felaktig e-postadress eller felaktigt lösenord"
"ac_modify_password" : "Ändra lösenord"
"ac_reset_password" : "Återställ lösenordet"
"ac_set_safe_password" : "Ange PIN-kod"
"ac_setup_password" : "Ange lösenord"
"base_agree_authority" : "Tillåt inte"
"base_apply_authority" : ""%1\$s" behöver tillgång till din %2\$s"
"base_auth_later" : "Auktorisera senare"
"base_auth_now" : "Auktorisera nu"
"base_authority_type" : "%1\$s myndighet"
"base_authorize" : "Auktorisera"
"base_engine_login_auth" : "Bekräftelse av inloggningen till fordonskontot"
"base_forget_password" : "Har du glömt ditt lösenord?"
"base_mysterious_user" : "Inga uppgifter"
"base_refuse_authority" : "OK"
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"permission_apply_authority" : ""%1\$s" behöver tillgång till din %2\$s"
"permission_authority_type" : "%1\$s myndighet"

"ve_auth_vehicle_account_login_tips" : "Vill du godkänna inloggningen på fordonskontot?"
"ac_account_login_with_password" : "התחברות באמצעות סיסמה"
"ac_account_password" : "סיסמה"
"ac_incorrect_email_or_password" : "דוא"ל או סיסמה שגויים"
"ac_modify_password" : "שינוי סיסמה"
"ac_reset_password" : "איפוס סיסמה"
"ac_set_safe_password" : "הגדרת קוד סודי"
"ac_setup_password" : "הגדרת סיסמה"
"base_agree_authority" : "אל תאפשר"
"base_apply_authority" : "שלך צריך הרשאת גישה ל-%2\$s" %1\$s"
"base_auth_later" : "אחר כך"
"base_auth_now" : "מתן הרשאות"
"base_authority_type" : "הרשאה %1\$s"
"base_authorize" : "אישור"
"base_engine_auth_success" : "ההרשאה הצליחה"
"base_engine_grant_auth" : "הרשאת התחברות לרכב"
"base_engine_login_auth" : "אשר התחברות רכב"

"base_forget_password" : "שכחת סיסמה?"
"base_mysterious_user" : "המשתמש הזה מאוד מסתורי"
"base_refuse_authority" : "אישור"
"com_facebook_device_auth_instructions" : "ולחצו את הקוד המוצג למעלה facebook.com/device יש לבקר בכתובת"
"permission_apply_authority" : ""%1\$s" %2\$s לגישה ל-"
"permission_authority_type" : "%1\$s של סמכות"
"ve_auth_vehicle_account_login_tips" : "האם ברצונך לאשר את ההתחברות לחשבון הרכב?"



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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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
	危		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

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
--------------	------------

com.gdc.ora.ui.AppLinkActivity	Schemes: comoragermany://, Hosts: app, Paths: /outlink.html,
com.gdc.ora.ui.MainActivity	Schemes: ora://, Hosts: app,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.ora.germany,
com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity	Schemes: lineauth://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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。