MoGua

VMOS Pro 2.5.0.APK 分析报告

APP名称: VMOS Pro

包名:	com.vmos.pro
域名线索:	9条
URL线索:	9条
邮箱线索:	1条
分析日期:	2024年4月25日
分析平台:	摸瓜反编译平台

文件信息

文件名: VMOS Pro永久会员.apk
文件大小: 27.96MB
MD5值: 511fd8c76a720bfe7d64b8a61a2dcd1e
SHA1值: be823ef52a893353b333b7f77f8da12e2e1e534b
SHA256值: 41b1d51b25cd6f014c4cfcfd2fe3d90bb792cacda61fedfa8c0935fa5d9a1e22

APP 信息

App名称: VMOS Pro
包名: com.vmos.pro
主活动Activity: com.vmos.pro.activities.splash.SplashActivity
安卓版本名称: 2.5.0
安卓版本: 20500

域名线索

域名	服务器信息
eco.taobao.com	**IP**: 59.82.31.115 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
opencloud.wostore.cn	**IP**: 210.22.123.92 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
	IP: 42.123.76.65 **所属国家**: China **地区**: Beijing

e.189.cn	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
wap.cmpassport.com	**IP**: 120.197.235.27 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.116671 **经度**: 113.250000
www.winimage.com	**IP**: 198.50.170.91 **所属国家**: Canada **地区**: Quebec **城市**: Beauharnois **纬度**: 45.316780 **经度**: -73.865898
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
www.qq.com	**IP**: 175.27.8.138 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
errlog.umeng.com	**IP**: 223.109.148.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

errlogos.umeng.com	**IP**: 47.246.110.18 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource
http://www.winimage.com/zLibDll	lib/armeabi-v7a/libnative-lib.so
https://wap.cmpassport.com/resources/html/contract.html	lib/armeabi-v7a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/armeabi-v7a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/armeabi-v7a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://eco.taobao.com/router/rest	lib/armeabi-v7a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so

https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
www.qq.com	lib/armeabi-v7a/libmarsstn.so
http://www.winimage.com/zLibDll	lib/arm64-v8a/libnative-lib.so
https://wap.cmpassport.com/resources/html/contract.html	lib/arm64-v8a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/arm64-v8a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/arm64-v8a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://eco.taobao.com/router/rest	lib/arm64-v8a/libauth_number_product-2.12.3.4-nolog-online-standard-channel_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so
www.qq.com	lib/arm64-v8a/libmarsstn.so

邮箱线索

邮箱地址	所在文件
ts@vmos.cn 发送邮件到ts@vmos.cn	Android String Resource

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: ST=HUNAN
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-21 11:17:58+00:00
Valid To: 2045-04-15 11:17:58+00:00
Issuer: ST=HUNAN
Serial Number: 0x48a78cc5
Hash Algorithm: sha256
md5: dead9c09203dd60eb4d1b885b8c13204
sha1: e2187ab11d1baeaa62317bd8fdcdfb85ce2c0931
sha256: 86f74d55cb495a8af927cd0607ae02fd53e7b260001753438cf2f89f8f5b3a1a
sha512: 8e9d9283215f2072b9f92098ac7d9fa5892ea3bee543016d45b0f7f80f47263097b1a32474736410325a62b2ba279a9394177128aa2641fc9beafc42e3b47ead
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 2c661f5b99f9c7a9671edcd841f170369266bed3cb70ebb3888098cc76b96c73

硬编码敏感信息

可能的敏感信息

"admire_author_pay_1" : "Give a gratuity to the author immediately%s"

"admire_author_pay_2" : "Choose%s, the expiration date is%s"

"boot_check_fingerprint_goto_password" : "Power-On By Password"

"common_go_auth" : "To authorize"

"defalut_user_name" : "VMOSPro User"

"default_user_name" : "VMOSPro用户"

"library_roundedimageview_author" : "Vince Mi"

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"password" : "Password"

"person_reply_user" : "%s 回复 %s :%s"

"reply_user" : "回复： %s"

"set_vmos_VirtualKey" : "Virtual Key"

"set_vmos_VirtualKey_detail" : "Three King Kong at the bottom of the virtual machine (multitasking, home screen, back)"

"set_vmos_boot_password" : "Power-on by password"

"set_vmos_virtual_key" : "Enable virtual buttons"

"setting_pwd1" : "Set new password"

"setting_pwd2" : "Test and verify"

"setting_pwd_1" : "Verification code has been sent to"

"setting_pwd_2" : "Verification code sent"
"setting_pwd_3" : "Cannot be the same as the old password"
"super_user" : "ROOT"
"admire_author_pay_1" : "立刻赞赏作者%s"
"admire_author_pay_2" : "选择%s，可使用至%s"
"boot_check_fingerprint_goto_password" : "密码开机"
"common_go_auth" : "去授权"
"defalut_user_name" : "VMOSPro 用户"
"default_user_name" : "VMOSPro用户"
"password" : "密码"
"person_reply_user" : "%s 回复 %s ：%s"
"reply_user" : "回复： %s"
"set_vmos_VirtualKey" : "虚拟按键"
"set_vmos_VirtualKey_detail" : "虚拟机底部三大金刚（多任务，主屏幕，返回）"
"set_vmos_boot_password" : "开机密码"
"set_vmos_virtual_key" : "启用虚拟按键"
"setting_pwd1" : "设置新密码"

"setting_pwd2" : "验证"
"setting_pwd_1" : "验证码已发送至"
"setting_pwd_2" : "验证码已发送"
"setting_pwd_3" : "不能与旧密码相同"
"super_user" : "超级用户"

加壳分析

加壳类型	所属文件
360	libjiagu.so
360	libjiagu_x86.so

第三方SDK

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_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.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.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.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.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_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.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.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.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.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.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.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.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of 指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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.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.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.SYSTEM_OVERLAY_WINDOW	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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
com.android.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.miui.home.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.miui.home.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.google.android.apps.nexuslauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

com.anddoes.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.lenovo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	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.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher2.permission.WRITE_SETTINGS	未知	Unknown	Unknown permission from android reference

		permission	
net.oneplus.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.oneplus.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.vmos.pro.openadsdk.permission.TT_PANGOLIN	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

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109614118://,
com.vmos.pro.activities.main.MainActivity	Schemes: rom://, Hosts: com.vmos.pro,
com.vmos.pro.utils.pay.QQPayCallbackActivity	Schemes: qwallet1109614118://,