MoGua

VMOS Pro 2.9.8.APK 分析报告

APP名称: VMOS Pro

包名:	VMOS Pro_2.9.8@RikkaTi.apk
域名线索:	4条
URL线索:	3条
邮箱线索:	1条
分析日期:	2025年6月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: VMOS Pro_2.9.8@RikkaTi.apk
文件大小: 32.63MB
MD5值: 1b80adf7ee75b699e9612397cca2e942
SHA1值: 9629318c89e104b740d7e40c27754525d954cd69
SHA256值: fb513905d24a0774dc9b588985195adde7690b621c856d2384a403fd016a5980

APP 信息

App名称: VMOS Pro
包名: VMOS Pro_2.9.8@RikkaTi.apk
主活动Activity: []
安卓版本名称: 2.9.8
安卓版本: 29008000

域名线索

域名	服务器信息
astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
github.com	**IP**: 192.30.255.112 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
vproapi.vmos.cn	**IP**: 39.103.168.8 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
astat.bugly.cros.wr.pvp.net	**IP**: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418

URL线索

URL信息	Url所在文件
https://vproapi.vmos.cn/	defpackage/da6.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://github.com/vinc3m1	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1

邮箱线索

邮箱地址	所在文件

xiaosuan@vmos.com ts@vmos.cn 发送邮件到ts@vmos.cn	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=CN
签名算法: rsassa_pkcs1v15
有效期自: 2021-02-13 12:15:19+00:00
有效期至: 2121-01-20 12:15:19+00:00
发行人: C=CN
序列号: 0xe6fcbbb
哈希算法: sha1
md5值: f9c489a84fa7b58c83a1596b726c88cf
sha1值: 792539cf2b9a9134d4b098472619e3ac2ffdd989
sha256值: f350e5f030a5298094935ee2bd0390dec2555ad16930cedfaadead6545d32abf
sha512值: a4ceebad322e1f58bbd7750288f7b174ac4f2d6f238be71811d9c79ea4ee470a6b84c65ecc5f4e9509a1cb7abdfa8b5373f7715b095c4f467e5a65911fb66672
公钥算法: rsa
密钥长度: 1024
指纹: 4dfdddf649063fc73f31ebd0b99380efbe1eb326bcca423305887b8ee340836c

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_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_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"

"admire_author_pay_1" : "Немедленно пожертвовать автору %s"

"admire_author_pay_2" : "Выберите %s, срок действия до %s"

"boot_check_fingerprint_goto_password" : "Парольный вход"

"common_go_auth" : "Авторизация"

"defalut_user_name" : "Пользователь VMOSPro"

"default_user_name" : "VMOSProПользователь"

"password" : "Пароль"

"person_reply_user" : "%s Re %s ：%s"

"reply_user" : "Re： %s"

"set_vmos_VirtualKey" : "Виртуальные клавиши"

"set_vmos_boot_password" : "Пароль запуска"

"set_vmos_virtual_key" : "Включить виртуальные кнопки"

"setting_pwd1" : "Установите новый пароль"

"setting_pwd2" : "Подтверждение пароля"

"setting_pwd_1" : "Код подтверждения отправлен на"

"setting_pwd_2" : "Код подтверждения отправлен"

"setting_pwd_3" : "Новый пароль не может быть таким же, как старый"
"super_user" : "Суперпользователь"

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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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	Unknown	Unknown permission from android reference

	知	permission	
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	Unknown	Unknown permission from android reference

	知	permission	
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 permission	Unknown permission from android reference
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.ACCESS_ALL_DOWNLOADS	未知	Unknown permission	Unknown permission from android reference
android.permission.HIGH_SAMPLING_RATE_SENSORS	正常	访问更高采样率的传感器数据	允许应用访问采样率大于 200 Hz 的传感器数据
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。

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://,

---