Evaluation Warning: The document was created with Spire.Doc for Python.

**VMOS（ 2.0.0-alpha01版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | VMOS |
| 版本 | 2.0.0-alpha01 |
| 包名 | com.vmos.openapp |
| 域名线索 | 21条 |
| URL线索 | 11条 |
| APP图标 |  |
| 分析日期 | 2024年10月18日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 2024052811002829001.apk |
| 文件大小 | 309.4MB |
| MD5值 | b7b1b408336034230a452581440ed5d5 |
| SHA1值 | 4abf04b548a32a3f0dc99980e43d1d608ba0194b |
| SHA256值 | 7ca340ad138e4e056df29f7bd5dc7fa04ee133a5c3f0c0560c51798fe0d739a1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | VMOS |
| 包名 | com.vmos.openapp |
| 主活动Activity | com.vmos.openapp.ui.SplashActivity |
| 安卓版本名称 | 2.0.0-alpha01 |
| 安卓版本 | 20001 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| me.cpatrk.net | IP: 116.198.14.137 所属国家: China 地区: Beijing 城市: Beijing  |
| openapp.vmos.cn | IP: 47.92.85.129 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.android.com | 没有服务器地理信息.  |
| api.talkingdata.com | IP: 116.196.64.97 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.bouncycastle.org | IP: 203.32.61.103 所属国家: Australia 地区: Victoria 城市: Drouin  |
| cloud.xdrig.com.td.fusion.iaas.jdcloud.com | IP: 116.198.14.27 所属国家: China 地区: Beijing 城市: Beijing  |
| cloud.cpatrk.net | IP: 116.198.14.43 所属国家: China 地区: Beijing 城市: Beijing  |
| 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  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| files.vmos.cn | IP: 202.108.29.174 所属国家: China 地区: Beijing 城市: Beijing  |
| service.vmos.com | IP: 104.26.5.148 所属国家: United States of America 地区: California 城市: San Francisco  |
| tdsdk.cpatrk.net | IP: 116.198.16.209 所属国家: China 地区: Beijing 城市: Beijing  |
| dns.qq.com | IP: 119.29.29.229 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| sx-common-v4.volcgtm.com | IP: 218.60.57.138 所属国家: China 地区: Liaoning 城市: Shenyang  |
| ins-9fciednc.ias.tencent-cloud.net | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| shouji.vmos.cn | IP: 218.60.57.138 所属国家: China 地区: Liaoning 城市: Shenyang  |
| shouji.vmos.cn.volcgslb.com | IP: 218.60.57.138 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.vmos.cn | IP: 47.92.89.32 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/b.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://cloud.cpatrk.net/configcloud/rest/sdk/gdprCheck  | com/tendcloud/tenddata/aa.java  |
| https://tdsdk.cpatrk.net/n/a/v1  | com/tendcloud/tenddata/aa.java  |
| https://cloud.cpatrk.net/configcloud/rest/sdk/match  | com/tendcloud/tenddata/aa.java  |
| https://me.cpatrk.net  | com/tendcloud/tenddata/a.java  |
| https://api.talkingdata.com/adt/openapi/rest/socialSharing/getShortUrl  | com/tendcloud/tenddata/bc.java  |
| https://api.talkingdata.com/adt/openapi/rest/socialSharing/getShortUrl?sign=  | com/tendcloud/tenddata/bc.java  |
| https://dns.qq.com  | com/tendcloud/tenddata/aj.java  |
| https://openapp.vmos.cn/api/  | com/vmos/openapp/a.java  |
| me.cpatrk.net  | 摸瓜V3引擎  |
| openapp.vmos.cn  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_8.png  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_2.png  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_4.png  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_12.png  | 摸瓜V3引擎  |
| cloud.xdrig.com.td.fusion.iaas.jdcloud.com  | 摸瓜V3引擎  |
| cloud.cpatrk.net  | 摸瓜V3引擎  |
| https://astat.bugly.qcloud.com/rqd/async  | 摸瓜V3引擎  |
| android.bugly.qq.com  | 摸瓜V3引擎  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_14.png  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto/com.android.launcher3  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_5.png  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://openapp.vmos.cn/api/  | 摸瓜V3引擎  |
| https://api.talkingdata.com/adt/openapi/rest/socialSharing/getShortUrl?sign=  | 摸瓜V3引擎  |
| tdsdk.cpatrk.net  | 摸瓜V3引擎  |
| https://dns.qq.com  | 摸瓜V3引擎  |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | 摸瓜V3引擎  |
| https://me.cpatrk.net  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_13.png  | 摸瓜V3引擎  |
| https://h.trace.qq.com/kv  | 摸瓜V3引擎  |
| sx-common-v4.volcgtm.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://www.bouncycastle.org  | 摸瓜V3引擎  |
| http://service.vmos.com/  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_6.png  | 摸瓜V3引擎  |
| ins-9fciednc.ias.tencent-cloud.net  | 摸瓜V3引擎  |
| shouji.vmos.cn  | 摸瓜V3引擎  |
| shouji.vmos.cn.volcgslb.com  | 摸瓜V3引擎  |
| http://files.vmos.cn/vmospro/picture/img\_bg\_10.png  | 摸瓜V3引擎  |
| www.vmos.cn  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| romex@romex.apk priv-app@romex\_cn.apk  | com/vmos/core/p0.java  |
| framework@boot.oat  | com/vmos/utils/c.java  |
| appro@openssl.org  | lib/arm64-v8a/libadb.so  |

### **4.4 手机号线索**

## **5. 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: CN=VMOS, OU=VMOS, O=VMOS, L=Changsha, ST=Hunan, C=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-25 10:45:05+00:00 有效期至: 2074-05-13 10:45:05+00:00 发行人: CN=VMOS, OU=VMOS, O=VMOS, L=Changsha, ST=Hunan, C=CN 序列号: 0x1 哈希算法: sha256 md5值: f3cdf1f0a906f1bfb6cc95b9484adf95 sha1值: 4a919b59f4e316aad8e8d37acdd9ab0aed70f86c sha256值: 9403d15076dfbfbd1587a91aec0a955aa71a813aa2593ab8e11e290b572ef683 sha512值: 493b9f882e1f4e2b69301f7de8ed4b0e73b95811021864f0dc59a9bf64b15e0cf63e821a86afa6b873093e512cdd7c9b498481ccdc86639c5bf825fbc5035053 公钥算法: rsa 密钥长度: 2048 指纹: efef3269f9d5cf20f3189862b97151fcaab48e8e1b53916777a9f39c51377b93**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.android.permission.GET\_INSTALLED\_APPS | 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.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\_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.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\_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\_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\_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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_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。 |
| 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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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 |
| com.vmos.openapp.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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.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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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 |
| 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.launcher.permission.READ\_SETTINGS | 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.android.launcher2.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.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.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 |
| 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.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.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.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。 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**