南明离火
移动应用检测平台

ANDROID 静态分析报告

录屏 • v8.28.888

分析日期: 2024-06-02 11:58:25

应用概览

文件名称:	com.michurou.screenrec_8.28.888.apk
文件大小:	50.96MB
应用名称:	录屏
软件包名:	com.michurou.screenrec
主活动:	com.rio.photomaster.SplashActivity
版本号:	8.28.888
最小SDK:	22
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	2/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	639380385a3086dbd0142b5c99cca659
SHA1:	b9d44972ed0194621855c68b[illegible]4534ede4cf
SHA256:	793b29e3145120fa90cdb1684e28410af020819e4[illegible]1a724500045cec86

分析结果严重性分布

高危	中危	信息	安全	关注
5	33	1	1	20

四大组件导出状态统计

Activity组件：102个，其中export的有： 16个
Service组件：13个，其中export的有： 3个
Receiver组件：1个，其中export的有： 0个
Provider组件：14个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=kankanscreen, ST=kankanscreen, L=kankanscreen, O=kankanscreen, OU=kankanscreen, CN=kankanscreen
签名算法: rsassa_pkcs1v15
有效期自: 2020-04-29 08:05:13+00:00
有效期至: 2045-04-23 08:05:13+00:00
发行人: C=kankanscreen, ST=kankanscreen, L=kankanscreen, O=kankanscreen, OU=kankanscreen, CN=kankanscreen
序列号: 0x23793a0b
哈希算法: sha256
证书MD5: 348fa89922498f4a64003a5716e402fd
证书SHA1: ad0f9d78c699f5c51217db3dff4f46c5ff371efe
证书SHA256: 5dba653f3be7befcd3d4a43c6025e49e3fd2498409be807538de322112dee339
证书SHA512:
9140218d80163bd9779844ac161f672545bfb4dc12604709c58afd00d42fddb559f8fe6aebd7e87df89faff9fba5b8114cf2c5403bd9c20fc74c27d778dd43fa

公钥算法: rsa
密钥长度: 2048
指纹: 4e08bf41fdb139e80e866bc7687483acd109b10719664afcee4ef92bc85bbc3c
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。

android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.MONITOR_POINTER_EVENT	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.ACCESS_UDID	未知	未知权限	来自 android 引用的未知权限。
com.xiaomi.permission.ACCESS_SECURITY_DEVICE_CREDENTIAL	未知	未知权限	来自 android 引用的未知权限。
com.samsung.android.rubin.context.permission.READ_CONTEXT_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.samsung.android.rubin.context.permission.WRITE_CONTEXT_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.miui.securitycenter.permission.ACCESS_SECURITY_CENTER_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.michurou.screenrec.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。

android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	Schemes: tencent101874820://,
com.thl.thl_advertlibrary.activity.Fhad_WebPageActivity	Schemes: https://, Hosts: ssl.ptlogin2.qq.com, Paths: /jump,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **1** | 警告: **23** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.1-5.1.1 [minSdk=22]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.rio.photomaster.ui.LoginActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

5	Activity (com.rio.photomaster.ui.MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Activity (com.tendory.screenrec.ScreenShotActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity设置了TaskAffinity属性 (com.michurou.screenrec.wxapi.WXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
8	Activity (com.michurou.screenrec.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity设置了TaskAffinity属性 (com.michurou.screenrec.wxapi.WXPayEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity (com.michurou.screenrec.wxapi.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Activity (com.tencent.tauth.AuthActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
12	App 链接 assetlinks.json 文件未找到 [android:name=com.thl.thl_advertlibrary.activity.Fhad_WebPageActivity] [android:host=https://ssl.ptlogin2.qq.com]	高危	App Link 资产验证 URL （https://ssl.ptlogin2.qq.com/.well-known/assetlinks.json）未找到或配置不正确。（状态代码：302）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify="true"] 启用验证来验证 App Link 网域。
13	Activity (com.thl.thl_advertlibrary.activity.Fhad_WebPageActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
14	Activity (com.mob.id.MobIDSYActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (com.mob.guard.MobTranPWLockActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Service (com.mob.MobACService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

17	Activity (com.mob.id.MobIDActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
18	Service (com.mob.id.MobIDService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
19	Activity (com.mob.guard.MobTranPullUpActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
20	Service (com.mob.guard.MobGuardPullUpService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
21	Activity (com.alipay.sdk.app.PayResultActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
22	Activity (com.alipay.sdk.app.AlipayResultActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
23	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityProxy) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
24	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityLiveProcessProxy) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
25	Activity (com.mob.tools.MobUIShell) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

代码安全漏洞检测

高危: **4** | 警告: **3** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限

3	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
7	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
8	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
9	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
10	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限

11	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
12	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
13	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
14	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	arm64-v8a/libavutil.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
2	arm64-v8a/libpostproc.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

3	arm64-v8a/librgb2yuv.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE android.permission.WRITE_SETTINGS android.permission.VIBRATE android.permission.READ_CONTACTS
其它常用权限	13/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.BLUETOOTH android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
loving.fanghenet.com	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图
download.sdk.mob.com	安全	是	**IP地址:** 45.113.201.237 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
apps.bytesfield.com	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
i.snssdk.com	安全	是	**IP地址:** 52.20.185.129 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
oss.fanghenet.com	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 河南 **城市:** 驻马店 **纬度:** 32.979439 **经度:** 114.030144 **查看:** 高德地图
identify.verify.mob.com	安全	是	**IP地址:** 103.143.17.149 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.sanyingapp.com	安全	否	**IP地址:** 52.31.24.56 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图

resource.sqcat.cn	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
jzvd.nathen.cn	安全	否	No Geolocation information available.
www.mob.com	安全	是	**IP地址:** 45.113.201.237 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
wx.tenpay.com	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224315 **经度:** 121.468948 **查看:** 高德地图
init.sms.mob.com	安全	是	**IP地址:** 103.143.17.149 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.chengzijianzhan.com	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
www.michurou.com	安全	是	**IP地址:** 47.92.233.19 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
browser.51star.top	安全	是	**IP地址:** 221.230.244.93 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图

sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 52.20.185.129 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
www.smpte-ra.org	安全	否	**IP地址:** 103.143.17.149 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.toutiaopage.com	安全	是	**IP地址:** 27.155.113.139 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
beian.miit.gov.cn	安全	是	**IP地址:** 27.155.113.139 **国家:** 中国 **地区:** 福建 **城市:** 福州 **纬度:** 26.061390 **经度:** 119.306107 **查看:** 高德地图
apps.bytesfield-b.com	安全	是	**IP地址:** 121.228.130.80 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.fangdingtech.cn	安全	是	**IP地址:** 47.92.233.19 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
apps.oceanengine.com	安全	是	**IP地址:** 121.228.188.228 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图

asoto.top	安全	是	**IP地址:** 47.92.95.145 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://asoto.top/aso/xm/upload_v2 • http://asoto.top/aso/sx/upload_v1 • http://asoto.top/aso/hw/upload_v1	cn/gz3create/args/v3/DynamicGetterXm.java
• data:/dev:/system/vendor/bin:/vendor/xbin:/system/vendor/xbin:/product/bin:/product/xbin:/data/local/tmp:/data/local/bin:/data/local/xbin:/data/local:/system/bin/failsafe	cn/gz3create/args/v3/GetXiaomiV3.java
• http://47.97.210.7:8920/real-data/v2 • http://47.97.210.7:8920/real-data/conn	cn/gz3create/args/v3/Gather.java
• http://jzvd.nathen.cn/c6e3dc12a1154626b3476d9bf3bd7266/6b56c5f0dc31428083775145764763b0-5287d2089db37e62345123a1be272f8b.mp4	com/tencory/whole/jiaozivideo/JZUtils.java
• https://loving.fanghenet.com • http://browser.51star.top:8080	apache/rio/kluas_update/AppConfig.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java

• 11.0.0.108 • 11.0.0.39 • 9.0.0.101 • 9.0.1.1 • 11.0.0.100 • 11.0.20.7 • 2.13.2.3 • 11.0.0.17 • 1.0.0.27 • 11.0.0.110 • 11.0.0.106 • 6.0.0.10 • 11.0.0.102 • 11.0.6.209 • 2.0.0.1 • 11.0.0.120 • 11.0.0.107 • 11.0.0.25 • 11.0.0.67 • 11.0.0.250 • 11.0.6.212 • 8.0.0.200 • 11.0.0.101 • 5.0.0.1 • 11.0.1.1 • 5.1.2.4 • 10.0.0.67 • 11.0.2.201 • 11.0.0.140 • 11.0.0.2 • data:/dev:/system/vendor/bin:/vendor/xbin:/system/vendor/xbin:/product/bin:/product/xbin:/data/local/tmp:/data/local/bin:/data/local/xbin:/data/local:/system/bin/failsafe • 11.0.1.102 • 10.0.0.102 • 11.0.0.113 • 11.0.0.3 • 11.0.1.113 • 3.1.0.28 • 8.0.0.203 • 5.1.2.10 • 11.0.0.200 • 11.0.0.1 • 11.0.0.134	cn/gz3create/args/v3/GetHuawei.java

• 3.3.23.33 • 1.1.35.1 • 5.1.15.1 • 2.1.37.2 • 1.1.13.37 • 2.0.12.1 • 10.0.40.36 • 2.1.30.4 • 1.1.32.2 • 10.0.16.14 • 5.0.22.8 • 1.1.26.1 • 10.1.30.16 • 8.1.80.2 • 3.1.29.1 • 2.1.13.6 • 1.6.24.50 • 1.0.57.8 • 2.6.30.1 • 7.0.18.1 • 10.1.30.5 • 6.3.47.66 • 1.0.0.2 • 2.9.13.9 • 1.0.11.92 • 3.0.12.9 • 10.2.30.33 • 10.1.51.21	cn/gz3create/args/v3/GetSamsung.java
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
• data:/dev:/system/vendor/bin:/vendor/xbin:/system/vendor/xbin:/product/bin:/product/xbin:/data/local/tmp:/data/local/bin:/data/local/xbin:/data/local:/system/bin/failsafe	cn/gz3create/args/v3/GetHuaweiV2.java
• http://www.michurou.com/privacy-lupin.html	com/rio/photomaster/ui/ListActivity.java
• http://www.baidu.com/s?&ie=utf-8&oe=utf-8&wd=	apache/rio/kluas_update/utils/ApplicationUtil.java
• https://wx.tenpay.com • https://d.alipay.com	com/thl/thl_advertlibrary/activity/Fhad_WebPageActivity.java
• https://resource.sqcat.cn/chat/imgs/ic_yonghu.png • http://oss.fanghenet.com/chat-client/index.html?user_id= • https://resource.sqcat.cn/chat/imgs/ic_kefu.png	com/rio/photomaster/ui/CustomerServiceActivity.java
• 127.0.0.1 • http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
• http://www.michurou.com/privacy-lupin.html	com/rio/photomaster/ui/PrivacyActivity.java
• http://www.fangdingtech.cn/agreement-lupin.html	com/rio/photomaster/ui/fragment/MineFragment.java
• https://mms.oceanengine.com/customer/api/app/pkg_info? • www.chengzijianzhan.com • www.toutiaopage.com/tetris/page	com/ss/android/downloadlib/addownload/compliance/lq.java

本报告由南明离火移动安全分析平台生成

• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• https://apps.bytesfield.com • https://apps.bytesfield-b.com	com/ss/android/downloadlib/addownload/compliance/sq.java
• http://www.fangdingtech.cn/privacy-lupin.html	com/rio/photomaster/ui/fragment/VipFragment.java
• 12.3.0.5 • 11.0.1.70 • 2.2.17.19 • 3.2.12.24 • 6.3.4.2 • 1.9.0.2 • 12.4.1.2 • 10.0.0.1 • 1.1.0.13 • 23.2.3.28 • 9.0.0.3 • 12.6.8.1 • 1.0.0.16 • 11.0.9.3 • 9.0.0.4 • 12.0.1.5 • 6.3.7.2 • data:/dev:/system/vendor/bin:/vendor/xbin:/system/vendor/xbin:/product/bin:/product/xbin:/data/local/tmp:/data/local/bin:/data/local/xbin:/data/local:/system/bin/failsafe • 12.0.0.21 • 12.0.0.6	cn/gz3create/args/v1/GetXiaomi.java
• http://browser.51star.top:8080	com/rio/photomaster/base/RootApp.java
• http://www.baidu.com	apache/rio/kluas_third/qq/QqConfig.java
• http://asoto.top/aso/xm/upload_v2 • http://asoto.top/aso/hw/upload_v2 • http://asoto.top/aso/sx/upload_v1	cn/gz3create/args/v3/DevicesGetter.java
• http://init.sms.mob.com/v3/sdk/init	cn/smssdk/utils/a.java
• http://www.mob.com/about/policy	cn/smssdk/utils/b.java
• http://identify.verify.mob.com/auth/verify/mobile	cn/smssdk/net/login/LoginCore.java

• http://download.sdk.mob.com/cc3/00e/dedc8bf1514d6c6a5e456fba74.png • http://download.sdk.mob.com/510/deb/0c0731ac543eb71311c482a2e2.png • http://download.sdk.mob.com/e31/c6e/315fdfa6abc4b17d8c139605de.png • http://download.sdk.mob.com/29f/06f/e6a941cd02e3f29465cd438d16.png • http://download.sdk.mob.com/167/bc4/38197ca7950aec7020d516fbb2.png • http://download.sdk.mob.com/7d7/e2b/91d898dfde6fb787ab3d926f9d.png • http://download.sdk.mob.com/f57/a5e/72ecd0c6ca96361c7f3bcd7144.png • http://download.sdk.mob.com/047/a51/38cfad789e9808443d11f2f9be.png • http://download.sdk.mob.com/7b6/264/2c4a9fef9ffa03e5deb5973ab9.png • http://download.sdk.mob.com/bbd/480/d993f23339944e4de27e4b0a12.png • http://download.sdk.mob.com/3a6/b11/ba6a81f2c13fb0ba3b96d99619.png • http://download.sdk.mob.com/e72/83d/e247e8b45bd557f70ac6dcc0cb.png • http://download.sdk.mob.com/cc6/115/2628761069dd35867eda68fe2a.png • http://download.sdk.mob.com/a0b/7d0/0520d3554a69ad50a3b87d1760.png • http://download.sdk.mob.com/d33/6f9/c15ee2d2f01aba51d33985e6c5.png • http://download.sdk.mob.com/f22/154/e27eaf3fc3e24047bd5d4ec3a8.png	cn/smssdk/gui/util/Const.java
• http://www.baidu.com/s?&ie=utf-8&oe=utf-8&wd=	com/thl/thl_advertlibrary/utils/Fhad_DeviceUtil.java
• https://loving.fanghenet.com	com/rio/photomaster/net/retrofit/RetrofitFactory_image.java
• https://loving.fanghenet.com	com/rio/photomaster/net/retrofit/RetrofitFactory_Buss.java
• 2.1.1.4	com/byted/live/api/BuildConfig.java
• https://beian.miit.gov.cn	com/rio/photomaster/ui/BeiAnActivity.java
• https://loving.fanghenet.com	com/rio/photomaster/net/retrofit/RetrofitFactory_AES.java
• http://www.michurou.com/privacy-lupin.html	com/rio/photomaster/ui/ThirdActivity.java
• http://www.michurou.com/agreement-lupin.html	com/rio/photomaster/ui/UserPrivacyActivity.java
• https://api.weixin.qq.com/sns/oauth2/access_token?grant_type=authorization_code&appid= • http://www.baidu.com • https://api.weixin.qq.com/sns/userinfo?access_token=	apache/rio/kluas_third/wx/WxConfig.java
• http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/k/hi.java
• http://www.mob.com • https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview • https://github.com/vinc3m1/roundedimageview.git	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息

本报告由南明离火移动安全分析平台生成

FFmpeg	FFmpeg	FFmpeg 是领先的多媒体框架，能够解码，编码，转码，MUX，DEMUX，流式，过滤和播放人类和机器创建的几乎所有内容。
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "5aa9ce167eddc7430000e4"
MobTech（袤博科技） 推送SDK的=> "Mob-AppKey" : "2f06a6fd6d32b"
MobTech（袤博科技） 推送SDK的=> "Mob-AppSecret" : "72c92f0ecc5fc823751f10759de7d528"
友盟统计的=> "UMENG_CHANNEL" : "yingyongbao"
"smssdk_authorize_dialog_reject" : "Disagree"
"smssdk_authorize_dialog_accept" : "Agree"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

11926ad43ab5c4d777d87a677c61ed22
A2B55680-6F43-11E0-9A3F-0002A5D5C51B
c6e3dc12a1154626b3476d9bf3bd7266
6b56c5f0dc31428083757a45764763b0-5287d2089db37e62345123a1be272f8b
ba6a81f2c13fb0ba3b96d99619
dedc8bf1514d6c6a5e456fba74
1ef570e1013109c50df8f8c2015faed71e4cf7c53ca9195a99c574ca046aeefdf70bc5fd69f04b0eadf63398698f776cf1ef0db5134efddc3aa4825b69aee94b55356a15d2a50a325ef7bd2d9efe15f3ac5d2303e0bdf5147b3d0fb5fa4fd1d5ea07fe1b45912ff9d7fe472136ff49cb1176f0492f9bc737ec7ccad132a5ce57
qVyObdyMO0gOhWxU33MfniOGYANgTjRtZrwFaG0YItY=
91d898dfde6fb787ab3d926f9d
72ecd0c6ca96361c7f3bcd7144
9A04F079-9840-4286-AB92-E65BE0885F95
38197ca7950aec7020d516fbb2
2c4a9fef9ffa03e5deb5973ab9
d993f23339944e4de27e4b0a12
38cfad789e9808443d11f2f9be
315fdfa6abc4b17d8c139605de
c35aba6cab2ecf11c77c911944e61f32
fa3acdf1b118fc26668bf72a70d60aa024ac6d72e4c5f0bb8f082bc384b38d4e6dd7d1b672467a19793c8f770c63f48b409e87f5787371789af40b95eae9867b9
e27eaf3fc3e24047bd5d4ec3a8
0c0731ac543eb71311c482a2e7
o0gr3Zuewf8OpyV42Q9Fnit3MU
e6a941cd02e3f2d465cd438d16
HW2cvdp0vkWjlUPWCe9XXv2E4YDUkmVfToG3SOkKqDg=
2628761069dd35867eda68fe2a
e247e8b45bd557f70ac6dcc0cb
edef8ba9-79d0-4dca-93c8-27dcd51d21ed
gfe+XR1rnFAtXlaxB0LzVroP9JsC0tUaMgOfZsYlems=
IaAPuAkDREGD4tPYwnUH0tHcYgp2GykATCvSpM2m+Wk=

0520d3554a69ad50a3b87d1760
c15ee2d2f01aba51d33985e6c5
sQdbX+sU0IdnB2wic5nAD5TnVd46A+H/5dqacw20lJU=

免责声明及风险提示: