南明离火
移动应用检测平台

ANDROID 静态分析报告

同步助手互传文件 • v1.0.1.1001

分析日期: 2025-04-03 19:45:34

应用概览

文件名称:	同步助手互传文件 v1.0.1.1001.apk
文件大小:	44.43MB
应用名称:	同步助手互传文件
软件包名:	com.travis.tbzshcwj
主活动:	com.universal.wifi.SplashActivity
版本号:	1.0.1.1001
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	5/432
杀软检测:	AI评估：非常危险，建议联系安全专家人工研判
MD5:	e2bc81318095a314806d611b207a0495
SHA1:	5927112ebd8be96e80c1fbe29a62d16b14b7f0a0
SHA256:	ef791ece900561bb015b0c57d2a0a9cd59b5bfa52065f889faf4b33e642fc3

分析结果严重性

高危	中危	信息	安全	关注
3	38	2	2	17

四大组件信息

Activity组件：170个，其中export的有： 26个
Service组件：15个，其中export的有： 0个
Receiver组件：6个，其中export的有： 0个
Provider组件：17个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: None
主题: CN=1, OU=1, O=1, L=1
签名算法: rsassa_pkcs1v15
有效期自: 2024-11-07 11:55:45+00:00
有效期至: 2049-11-01 11:55:45+00:00
发行人: CN=1, OU=1, O=1, L=1
序列号: 0x1
哈希算法: sha256
证书MD5: a4a840567e7921511a76134c12c2c9cc
证书SHA1: 74137ae0e4716f743c815bacebbcfcd22e2b79c9
证书SHA256: e7b56a89bc3e222e2c92ccc4931fd34d8ffcba7cc2c8d01b099fb6a2d59e6178
证书SHA512:
ce882bb3b81fa3b6c47e8aeb049ba482d9a6a23fe1888cb209337894f5686d12d48c7231c00964246611744e09339b3d6c3cfd3d2eef49f4f0cd40163b6262b

公钥算法: rsa
密钥长度: 2048
指纹: 8ceb1ee3462803717d909905d6d9dc5da5b2a6a14d70e7e866b59e2c780d997a
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
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.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.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粗略的经纬度信息，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_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，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.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.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_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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.NEARBY_WIFI_DEVICES	危险	需要通过 Wi-Fi 进行广告和连接到附近的设备	需要能够通过 Wi-Fi 进行广告宣传和连接到附近的设备。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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。
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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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。
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。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
freemme.permission.msa.SECURITY_ACCESS	未知	未知权限	来自 android 引用的未知权限。
oplus.permission.settings.LAUNCH_FOR_EXPORT	未知	未知权限	来自 android 引用的未知权限。

com.vivo.identifier.permission.OAID_STATE_DIALOG	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
com.android.permission.GET_INSTALLED_APPS	未知	未知权限	来自 android 引用的未知权限。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
com.travis.tbzshcwj.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
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。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: **0** | 警告: **0** | 信息: **1**

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

MANIFEST分析

高危: **1** | 警告: **7** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	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。
2	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	Activity (com.universal.wifi.main.ui.main.splash.SplashActivityLater) 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。
4	Activity (com.universal.wifi.main.ui.main.MainActivity) 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。
5	Activity (com.universal.wifi.main.ui.main.splash.DeleteSplashActivityLater) 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。
6	Activity (com.universal.wifi.safe_ui.SafeMainActivity) 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 (com.universal.wifi.safe_ui.pre.SafePreSelectFileActivity) 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。
8	Activity (com.universal.wifi.home.send.SendSelectFileActivity) 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 (com.universal.wifi.home.ConnectActivity) 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。
10	Activity (com.universal.wifi.home.send.TransmittingActivity) 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.universal.wifi.home.send.SendFinishActivity) 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。
12	Activity (com.universal.wifi.home.pre.PreSelectFileActivity) 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。

本报告由南明离火移动安全分析平台生成

13	Activity (com.universal.wifi.home.accept.PhoneBrandActivity) 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。
14	Activity (com.universal.wifi.home.sweep.SweepActivity) 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.universal.wifi.home.accept.AcceptTransmittingActivity) 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	Activity (com.universal.wifi.home.accept.AcceptFinishActivity) 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。
17	Activity (com.universal.wifi.home.accept.AcceptAppsActivity) 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	Activity (com.universal.wifi.home.permission.PermissionMangerActivity) 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。
19	Activity (com.universal.wifi.home.FAQActivity) 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	Activity (com.universal.wifi.photo.speedySort.SpeedySortingActivity) 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。
21	Activity (com.universal.wifi.photo.speedySort.SpeedySortResultActivity) 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.universal.wifi.photo.recycleBin.RecycleBinActivity) 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.universal.wifi.photo.screenshot.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。
24	Activity (com.universal.wifi.photo.resemblance.ResemblanceActivity) 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.universal.wifi.photo.vague.VaguePhotoActivity) 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。
26	Activity (com.universal.wifi.notification.NotificationRouterActivity) 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。
27	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。
28	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。

</> 安全漏洞检测

高危: **1** | 警告: **10** | 信息: **2** | 安全: **2** | 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	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
3	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
4	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

5	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
6	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
7	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
8	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
9	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
10	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
12	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
13	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

14	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
15	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

动态库分析

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/libantitrace.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__vsprintf_chk']	True info 符号被剥离

本报告由南明离火移动安全分析平台生成

2	arm64-v8a/libavmdl_lite.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	True info 符号被剥离
3	arm64-v8a/libEncryptorP.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 符号被剥离

4	arm64-v8a/libglide-webp.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	True info 符号被剥离
5	arm64-v8a/libmaparmor.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 符号被剥离

6	arm64-v8a/libpanglearmor.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__strlen_chk', '__read_chk', '__vsprintf_chk', '__strcpy_chk']	True info 符号被剥离
7	arm64-v8a/libPglbizssdk_ml.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__vsprintf_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

8	arm64-v8a/libplt-base.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__read_chk', '__vsnprintf_chk', '__strlcpy_chk', '__strchr_chk', '__strlen_chk', '__strcpy_chk', '__strncpy_chk', '__memmove_chk']	True info 符号被剥离
9	arm64-v8a/libscore.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 符号被剥离

10	arm64-v8a/libsgcore.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	True info 符号被剥离
11	arm64-v8a/libti-monitor.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__memcpy_chk', '__vsnprintf_chk', '__memset_chk', '__strlen_chk']	True info 符号被剥离

12	arm64-v8a/libttmplayer_lite.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	True info 符号被剥离
13	arm64-v8a/libtt_ugen_yoga.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info 符号被剥离

行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限

00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限

00031	检查当前正在运行的应用程序列表	反射 信息收集	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00131	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 WiFi	升级会员：解锁高级权限
00135	获取当前WiFi id并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限

00099	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00113	获取位置并将其放入 JSON	信息收集 位置	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00044	查询该包的activity上次被使用的时间	信息收集 反射	升级会员：解锁高级权限
00045	查询当前运行的应用程序名称	信息收集 反射	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	19/30	android.permission.WRITE_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_SMS android.permission.WRITE_CALL_LOG android.permission.READ_CALL_LOG android.permission.SEND_SMS android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.PACKAGE_USAGE_STATS

其它常用权限	16/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.FLASHLIGHT android.permission.CHANGE_NETWORK_STATE com.google.android.gms.permission.AD_ID android.permission.REORDER_TASKS android.permission.FOREGROUND_SERVICE com.android.launcher.permission.INSTALL_SHORTCUT

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。

域名检测

域名	状态	中国境内	位置信息
wifi.kykeji.cn	安全	是	**IP地址:** 223.109.148.141 **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
apmplus.volces.com	安全	是	**IP地址:** 61.147.168.157 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
apps.bytesfield.com	安全	是	**IP地址:** 223.109.148.141 **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
journeyapps.com	安全	否	**IP地址:** 216.137.39.6 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 180.97.251.193 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
apps.bytesfield-b.com	安全	是	**IP地址:** 121.228.130.192 **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
api.xiaozhuowuxian.com	安全	是	**IP地址:** 180.97.251.193 **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
log.kykeji.cn	安全	是	**IP地址:** 180.97.251.193 **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
gator.volces.com	安全	是	**IP地址:** 180.97.251.193 **国家:** 中国 **地区:** 江苏 **城市:** 盐城 **纬度:** 33.385559 **经度:** 120.125282 **查看:** 高德地图
apmlog.snssdk.com	安全	是	**IP地址:** 180.97.251.193 **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
apps.oceanengine.com	安全	是	**IP地址:** 121.228.130.194 **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
yumao.pusta.info	安全	是	**IP地址:** 180.97.251.193 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图

gwaj71c5q1.feishu.cn	安全	是	**IP地址:** 183.61.169.132 **国家:** 中国 **地区:** 广东 **城市:** 东莞 **纬度:** 23.048780 **经度:** 113.745003 **查看:** 高德地图
xiaozhuowuxian.com	安全	是	**IP地址:** 114.112.25.147 **国家:** 中国 **地区:** 辽宁 **城市:** 大连 **纬度:** 41.069592 **经度:** 122.598511 **查看:** 高德地图
i.snssdk.com	安全	是	**IP地址:** 180.97.251.193 **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.chengzijianzhan.com	安全	是	**IP地址:** 180.97.251.193 **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.lrping123.apk	安全	否	No Geolocation information available.
www.samsungapps.com	安全	否	**IP地址:** 54.229.225.161 **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
www.toutiaopage.com	安全	是	**IP地址:** 121.228.130.196 **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
log.xiaozhuowuxian.com	安全	是	**IP地址:** 121.228.130.196 **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链接分析

URL信息	源码文件

• https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake_text.png • https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/swipe_right.webp • https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake.webp	自研引擎-A
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
• 2.10.42.103	com/bykv/vk/component/ttvideo/player/TTVersion.java
• https://log.xiaozhuowuxian.com/reporter/ • https://api.xiaozhuowuxian.com/cash/	com/universal/wifi/service/config/ServiceConfigBuilder.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/VideoLiveManager.java
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/of/jk.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/log/LiveLoggerService.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/BuildConfig.java
• 127.0.0.1	com/lahm/library/SecurityCheckUtil.java
• http://127.0.0.1	com/bykv/vk/component/ttvideo/DataLoaderHelper.java
• 127.0.0.1	com/lahm/library/VirtualApkCheckUtil.java
• https://%s/q?host=%s	com/bykv/vk/component/ttvideo/network/DnsHelper.java
• http://xiaozhuowuxian.com/wifiysqnmfl/ • https://log.xiaozhuowuxian.com/reporter/ • https://api.xiaozhuowuxian.com/cash/ • https://api.xiaozhuowuxian.com/hf/	com/universal/wifi/config/TemplateModuleConfigBuilder.java
• https://api.xiaozhuowuxian.com/cash/ • https://gwaj71c5q1.feishu.cn/share/base/form/shrcndlveeanxwhnoklabhvoua • https://log.xiaozhuowuxian.com/reporter/ • http://xiaozhuowuxian.com • https://log.xiaozhuowuxian.com • https://api.xiaozhuowuxian.com • http://xiaozhuowuxian.com/tbzshcwj/base.apk • http://xiaozhuowuxian.com/tbzshcwj/ • https://api.xiaozhuowuxian.com/hf/	com/universal/wifi/AppConfigImp.java
• https://api.xiaozhuowuxian.com/cash/	com/universal/wifi/App.java
• https://wifi.kykeji.cn/cash/ • https://log.kykeji.cn/reporter/	com/universal/wifi/service/ServiceModule.java
• 2.10.42.103	com/bykv/vk/component/ttvideo/port/BuildConfig.java
• https://apmlog.snssdk.com/apm/collect/crash/ • https://apmplus.volces.com/monitor/collect/c/session	com/bytedance/b/c/dj/c.java
• https://yumao.puata.info/cc_info	com/uyumao/d.java

• https://yumao.puata.info/anti_logs	com/uyumao/c.java
• http://127.0.0.1	com/bykv/vk/component/ttvideo/medialoader/MediaLoaderWrapper.java
• www.toutiaopage.com/tetris/page • www.chengzijianzhan.com • https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/c.java
• https://apps.bytesfield-b.com • https://apps.bytesfield.com	com/ss/android/downloadlib/addownload/compliance/bi.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• 1.1.37.41	com/bykv/vk/component/ttvideo/mediakit/medialoader/BuildConfig.java
• www.lrping123.apk	com/universal/wifi/audit/impl/SpecialAppCondition.java
• https://gator.volces.com	com/universal/wifi/pub/logger/VolcanoLoggerTracker.java
• https://yumao.puata.info/cc_info	com/uyumao/r.java
• https://github.com/journeyapps/zxing-android-embedded • https://journeyapps.com/	自研引擎-S
• 127.0.0.1 • 1.1.37.41 • tcp://%s	lib/arm64-v8a/libavmdl_lite.so
• data:%p,width:%d,height:%d,stride:%d,ret:%d • 2.10.42.103	lib/arm64-v8a/libttmplayer_lite.so

第三方SDK

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
EasyProtector	lamster2018	一行代码检测 XP/调试/多开/模拟器/root。
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。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
C++ 共享库	Android	在 Android 应用中运行原生代码。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
GlideWebpDecoder	zjupure	GlideWebpDecoder 是一个 Glide 集成库，用于在 Android 平台上解码和显示 webp 图像。它基于 libwebp 项目，并以 Fresco 和 GlideWebpSupport 的一些实现作为参考。

MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
OpenCV	OpenCV	OpenCV 是一个跨平台的计算机视觉库，可用于开发实时的图像处理、计算机视觉以及模式识别程序。
阿里聚安全	Alibaba	阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。
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。
移动应用推广 SDK	Baidu	百度移动推广 SDK(Android)是百度官方推出的移动推广 SDK 在 Android 平台上的版本
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。
DataFinder	Volcengine	基于灵活高效的分析模型，发现用户行为数据的价值，进而转化为促进增长的行动。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
快手广告 SDK	快手	快手信息流广告，为您和用户搭建桥梁。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
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 App Startup	Google	App Startup 库提供了一种直接、高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

追踪器

名称	类别	网址
Baidu Mobile Ads		https://reports.exodus-privacy.eu.org/trackers/100
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

密钥凭证

可能的密钥
"library_zxingandroidembedded_author" : "JourneyApps"
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

af4a94c58b3fda0506b817145ba1a146a1e7f3734965e75fa9a8d11d9eb13a33
682A27E934254A3B97FC65CF93601583e955ed413fa40a3c49b4fc364cd82cea
4ab312f7094810afa84659d3dc6cf0fe
eb3c2837-d2fc-4e41-a85a-283531e69723
30e5bbde-7e07-4403-ae08-1f1ab7e4924a
6563938d4d40a7917c3fa9480ca40919eabc937943ba8a3f5dbd7f784e58d960
87618845243B469DB9743541F56F971Aa81ef208eca3f9de0ad756d3f5cf23ac
d3ad8f81-833f-4104-a6d0-ddc5c40a61cd
E2A51D8769C74761ADE2214D7BF1932E17491c8e88347dfb137caaca3b0d2489
F467FDED3EBE41D78B10BD1B4DE27872e93f101abb1061c4631ae1147ad1d9af
A73BFFA340B5B650A7FBFFA2AB94C0E403DE71801EC31B13F7B584DCCC286B14
ce1f7301-a557-48ad-b88b-6c15868a4d32
C9F6BB45E9BB46D69F8B6E386D62B4C2e955ed413fa40a3cba192ea4e1307e66
2956816f-54fe-459a-aff8-9155d0296b25
96d7805c-b716-4fe0-b76f-d8c945d8dfa7
2D051579D2D34EA4A52272655190657380fe09864ea30f2b70772eb3dc1fd275
678f41859a16fe6dcd33e743
26C1573581F248ACABC9E328C9649833ea8c3c468166a2824132d376ff528c7b
5f43b9ac0d69148f6ae0fb3ad9f385d392635ea[illegible]2e954[illegible]30ab6c6146c6af1e0[illegible]

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。