南明离火
移动应用检测平台

ANDROID 静态分析报告

掌运达 v1

分析日期: 2025-08-29 11:12:53

应用概览

文件名称:	123.apk
文件大小:	85.01MB
应用名称:	掌运达
软件包名:	com.xianyi.mobile.dtxyzyd
主活动:	io.dcloud.DTXYActivity
版本号:	1
最小SDK:	21
目标SDK:	30
加固信息:	360加固
开发框架:	DCloud, Weex
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	7/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	688d68c1f01df0affa705b0e10bb5d3b
SHA1:	8450f7c5ef94e2a[illegible]d196[illegible]c2501f2485be[illegible]818
SHA256:	7c6db0502[illegible]b[illegible]b3[illegible]30d6e9240e3443[illegible]e[illegible]5e[illegible]793c57bf26904fb5e4ce7e758d3

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
3	24	1	1	0

四大组件导出状态统计

Activity组件：37个，其中export的有： 5个
Service组件：16个，其中export的有： 2个
Receiver组件：9个，其中export的有： 5个
Provider组件：6个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=Chine, ST=HuNan, L=Unknown, O=Hunan Datang Xianyi Technolocy Co., Ltd., OU=Hunan Datang Xianyi Technolocy Co., Ltd., CN=zhang
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-25 15:31:50+00:00
有效期至: 2051-12-11 15:31:50+00:00
发行人: C=Chine, ST=HuNan, L=Unknown, O=Hunan Datang Xianyi Technolocy Co., Ltd., OU=Hunan Datang Xianyi Technolocy Co., Ltd., CN=zhang
序列号: 0x18bee0ef
哈希算法: sha256
证书MD5: 67f39efb285db648a4608286f338fe8b
证书SHA1: 8f953026ae1ddbb768293db0ece2fc5061a37513
证书SHA256: 311d9d8f38a3c8387f732c4ecc1eb15a82e3fa72d0ce168a49447c38e3d19dbe
证书SHA512:
3aba052a23b347a03f6f28918d70e46d0e71b75853d453f9dc6da8405898fb994da145b508834c45504c[illegible]80bedd91ded508fe[illegible]489e69ff341a

公钥算法: rsa
密钥长度: 2048
指纹: 33892197295585105e47ca2a5af48e2231e6e747712016968c35822e85438d02
共检测到 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.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.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.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.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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.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.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.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_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.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.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.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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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。
getui.permission.GetuiService.com.xianyi.mobile.dtxyzyd	未知	未知权限	来自 android 引用的未知权限。
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。
com.xianyi.mobile.dtxyzyd.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.xianyi.mobile.dtxyzyd.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.xianyi.mobile.dtxyzyd.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.xianyi.mobile.dtxyzyd.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
com.xiaomi.permission.AUTH_SERVICE	未知	未知权限	来自 android 引用的未知权限。

本报告由南明离火移动安全分析平台生成

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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取设备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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.DTXYActivity	Schemes: gtpushscheme://, Hosts: com.getui.push, Paths: /detail,
com.tencent.tauth.AuthActivity	Schemes: 1104455702://,
io.dcloud.PandoraEntryActivity	Schemes: h56131bcf://,

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Activity (com.tencent.tauth.AuthActivity) 未受保护。存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
3	Broadcast Receiver (com.igexin.sdk.PushReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该Broadcast Receiver 被显式导出，存在安全风险。
4	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.PushActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.GActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
6	Activity 设置了 TaskAffinity 属性 (com.xianyi.mobile.dtxyzyd.wxapi.WXPayEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
7	Activity (io.dcloud.PandoraEntryActivity) 受权限保护，但应检查权限保护级别。Permission: com.miui.securitycenter.permission.AppPermissionsEditor [android:exported=true]	警告	检测到 Activity 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
8	Broadcast Receiver (com.igexin.sdk.HmsPushReceiver) 受权限保护，但应检查权限保护级别。Permission: com.xianyi.mobile.dtxyzyd.permission.PROCESS_PUSH_MSG protectionLevel: signature|system [android:exported=true]	信息	检测到 Broadcast Receiver 已导出并受权限保护，但权限保护级别为 signatureOrSystem。建议使用 signature 级别，避免依赖系统安装位置。

9	Broadcast Receiver (com.igexin.sdk.HmsPushSubReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
10	Broadcast Receiver (com.meizu.cloud.pushsdk.SystemReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
11	Broadcast Receiver (com.igexin.sdk.FlymePushReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
12	Service (com.igexin.sdk.OppoPushService) 受权限保护，但应检查权限保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
13	Service (com.igexin.sdk.OppoAppPushService) 受权限保护，但应检查权限保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
14	Broadcast Receiver (com.igexin.sdk.VivoPushMessageReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
15	Activity (com.alipay.sdk.app.PayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
16	Activity (com.alipay.sdk.app.AlipayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
17	Activity (com.sina.weibo.sdk.share.ShareTransActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **2** | 警告: **7** | 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	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
3	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
4	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
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	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	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
8	应用程序使用带PKCS5/PKCS7填充的加密模式 CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

9	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
10	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
11	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

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/libenc.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	False warning 符号可用
2	arm64-v8a/liblamemp3.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/libTRAECodec.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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
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
00024	Base64解码后写入文件	反射 文件	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
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
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
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
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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限

00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	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
00003	将压缩后的位图数据放入JSON对象中	相机	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
00012	读取数据并放入缓冲流	文件	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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
00088	创建到给定主机地址的安全套接字连接	命令 网络	升级会员：解锁高级权限
00148	创建到给定主机地址的套接字连接	网络 命令	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	15/30	android.permission.CAMERA android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WRITE_SETTINGS android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.GET_TASKS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.GET_ACCOUNTS

其它常用权限	10/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE

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
www.videolan.org	安全	否	**IP**地址: 213.36.253.2 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
• http://kjur.github.io/jsrsasign/api/symbols/KJUR.crypto.Mac.html • https://weibo.com/signup/v5/privacy?sbm=a1zaa.8161610.0.0.4f877621Wu8R1 • http://219.141.254.166:9000/mobile-api • http://fontello.com • https://tools.ietf.org/html/rfc7638 • https://tools.ietf.org/html/rfc2253 • http://www.secg.org/download/aid-780/sec1-v2.pdf • https://github.com/kjur/jsrsasign/wiki/NOTE-distinguished-name-representation-in-jsrsasign • http://offline-data.alicdn.com/amap/offlinemap/poi/unifyCompile/0TO3_18_01_08_00/a310.zip • https://api.weixin.qq.com/card/invoice/reimburse/getinvoicebatch?access_token • https://github.com/openpgpjs/openpgpjs/blob/master/LICENSE • http://ocsp.roo.com • http://example.org/aaa.crl • http://kjur.github.io/jsrsasign/license • http://www.github.com/kjur • http://rep.foo.com/aaa.p8m • http://kjur.github.com/jsrsasigns • https://tools.ietf.org/html/rfc2986 • https://ydyy004.china-cdt.com/mobile-api • https://github.com/openpgpjs/openpgpjs/blob/master/src/ciphers/asymmetric/dsa.js • http://a.com • http://124.232.157.38:90/mobile-api • http://bbb.com • https://tools.ietf.org/html/rfc7519 • https://github.com/bitcoinjs/bitcoinjs-lib	

• https://github.com/openpgpjs/openpgpjs/blob/master/src/util/util.js • https://github.com/openpgpjs/openpgpjs/blob/master/src/ciphers/openpgp.crypto.js • http://dev.dcloud.net.cn/mui • https://cdn.bootcdn.net/ajax/libs/vConsole/3.9.0/vconsole.min.js • https://tools.ietf.org/html/rfc5652 • http://foo.com • https://kjur.github.io/jsrsasign/sample/tool_jwktp.html • http://10.50.134.40:1089/mobile-api • http://aaa.com • http://developer.yahoo.com/yui/license.html • http://www-cs-students.stanford.edu • http://kjur.github.com/jsjws/license • http://www.owasp.org/index.php/XSS_ • https://ydyy001.china-cdt.com/mobile-api • http://kjur.github.com/jsjws • https://www.dtxytech.com • http://www.jonllen.com • http://ocsp.cacert.org • http://aaa.com/a.crl • http://blog.livedoor.jp/k_urushima/archives/656114.html • https://github.com/bitcoinjs/bitcoinjs-lib/blob/master/LICENSE • http://self-issued.info/docs/draft-jones-json-web-signature-04.html • http://kjur.github.io/jsrsasign/api/symbols/KJUR.crypto.Signature.html • http://kjur.github.com/jsrsasign • https://www.vivo.com.cn/about-vivo/privacy-policy • http://offlinedata.alicdn.com/amap/offlinemap/poi/unifyCompile/0TO3_18_01_08_00_a149.zip • http://www.ietf.org/mail-archive/web/jose/current/msg02901.html • https://tools.ietf.org/html/rfc5126 • https://tools.ietf.org/html/rfc6960 • https://tools.ietf.org/html/rfc7517 • http://192.168.23.129/mobile-api • http://www.dtxytech.com • http://tools.ietf.org/html/draft-jones-json-web-signature-json-serialization-01 • http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms-14 • https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy • https://crypto-js.googlecode.com/svn-history/r667/branches/3.x/src/core.js • https://github.com/bitcoinjs/bitcoinjs-lib/blob/master/src/ecdsa.js • http://perfectionkills.com/global-eval-what-are-the-options • http://kjur.github.com/jsrsasign/license • https://tools.ietf.org/html/rfc3161	自研引擎-A
• http://openapi.baidu.com/oauth/2.0/token?grant_type=client_credentials&client_id=	com/baidu/aip/core/mini/AutoCheck.java
• http://www.videolan.org/x264.html	lib/arm64-v8a/libenc.so

第三方 SDK 组件分析

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。
语音识别 SDK	Baidu	百度语音开放平台 Android SDK，提供短语音识别、实时语音识别、离线自定义命令词识别、远场语音识别、语音唤醒、语义解析与对话管理等相关接口。SDK内部均为采用流式协议，即用户边说边处理。区别于 Restapi 需要上传整个录音文件。

Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
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。
DCloud	数字天堂	libdeflate is a library for fast, whole-buffer DEFLATE-based compression and decompression.
FreeType	FreeType	FreeType 是免费提供的用于渲染字体的软件库。 它用 C 语言编写，旨在小巧、高效，高度可定制和便携式，同时能够生成大多数矢量和位图字体格式的高质量输出（字形图像）。
GCanvas	Alibaba	GCanvas 是一个跨平台的画布解决方案，它实现了图形 2D 和 WebGL API。GCanvas 使其用户能够直接访问 OpenGL ES API。GCanvas 旨在解决 JavaScript 开发人员的画布的性能问题和兼容性问题。
个推	个推	SDK 快速集成，免费注册使用。智能推送+场景推送，有效提升用户活跃度与粘性。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your TV too.
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
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。
腾讯云短视频 SDK	Tencent	腾讯云点播发出的短视频一站式解决方案，覆盖了视频生成、上传、处理、分发和播放在内的各个环节，帮助用户以最快速度实现短视频应用的上线。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
腾讯云直播 SDK	Tencent	云直播（Cloud Streaming Services，CSS）依托腾讯强大的技术平台，将腾讯视频等核心业务底层能力开放给用户，为用户提供专业稳定快速的直播接入和分发服务，具有低延迟、高安全、高性能、易接入、多终端、多码率支持等特点。
微博 SDK	Weibo	微博 Android 平台 SDK 为第三方应用提供了简单易用的微博 API 调用服务，使第三方客户端无需了解复杂的验证机制即可进行授权登陆，并提供微博分享功能，可直接通过微博官方客户端分享微博。
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
腾讯云实时音视频	Tencent	腾讯实时音视频（Tencent Real-Time Communication，TRTC），将腾讯 21 年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
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。
Weex	Alibaba	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验，来构建 Android、iOS 和 Web 应用。简单来说，在集成了 WeexSDK 之后，你可以使用 JavaScript 语言和前端开发经验来开发移动应用。

libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现对各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
HMS Update	Huawei	用于 HMS SDK 引导升级 Huawei Mobile Services(APK)，提供给系统安装器读取升级文件。
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。
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。
OPPO Push	OPPO	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

第三方追踪器检测

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
vivo推送的=> "com.vivo.push.app_id" : "105159017"
UniPush推送的=> "MIPUSH_APPKEY" : "XM_5531863023258"
QQ授权的=> "QQ_APPID" : "1104455702"
UniPush推送的=> "MEIZUPUSH_APPID" : "MZ_134319"
百度语音识别的=> "com.baidu.speech.APP_ID" : "11770490"
DCloud（数字天堂）的=> "dcloud_appkey" : "1764e9eac73c20a85ee33127abbff576"
百度语音识别的=> "com.baidu.speech.SECRET_KEY" : "vZK4rC7ueQTMrhavm3qVlnGicPTeUCEr"
小米分享的=> "MIUI_APPID" : "_%小米分享的APPID%"
新浪微博分享的=> "SINA_APPKEY" : "_3662743235"
UniPush推送的=> "OPPOPUSH_APPSECRET" : "OP_77fc1fb158c741c3ac45b04b79f35c17"
友盟统计的=> "UMENG_CHANNEL" : "googleplay"
个推-推送服务的=> "PUSH_APPKEY" : "vSewtjCvlb5ajJV2NxNjI8"
新浪微博分享的=> "SINA_SECRET" : "b8fa3ec4b7e47a152044d9e8265cf593"
个推-推送服务的=> "PUSH_APPID" : "JHbvDj1idZ6tXUz3ZqpSc9"
小米分享的=> "MIUI_APPSECRET" : "%小米分享的appSecret%"
高德地图的=> "com.amap.api.v2.apikey" : "1245f55df04583e53eb0fbf511be9a08"
个推-推送服务的=> "PUSH_APPSECRET" : "iKrS9W94bm8mSOumn4Pg83"
UniPush推送的=> "MEIZUPUSH_APPKEY" : "MZ_410863e5b044c6fbef878f26d5b2aab"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=103393953"
友盟统计的=> "UMENG_APPKEY" : "55b1b625e0f55a738300449d"
vivo推送的=> "com.vivo.push.api_key" : "21938ad4f5f311e5314564a43b0df8a"
UniPush推送的=> "OPPOPUSH_APPKEY" : "OP_6f38a3573a2c4ff48ec29321da3e2e63"
UniPush推送的=> "MIPUSH_APPID" : "XM_2882303761518630258"
凭证信息=> "IFLY_APPKEY" : "53eacdd"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "NkQUU5hdGVmKCDpWyp7Kp3j1gFlm4k5L"
百度语音识别的=> "com.baidu.speech.API_KEY" : "cDFRHjbhBklzS1ZKFBnz9cHg"
"app_id" : "H5EF97D4F"
"dcloud_permissions_reauthorization" : "reauthorize"

"dcloud_feature_oauth_weixin_plugin_description" : "wechat"
30820122300d06092a864886f70d01010105000382010f003082010a0282010100c54db230ca0e0f37b105a3cd364dd20c76d3574a781f884aeb7d7548fb33928eaafe7cf9d94b3dcb553bbb9e61821738b359da9f8cf1e9281cfbf84
49cb4254efce57d5861aedca86e5baf1205b09cd7f742b38065559f0f70676754915acca5ad6eeaa0d68dfd5143d0a50faedb6cda3b13852705c881ba5b587ecbbb4467cbed08b6754a3f424d90c66fd3b82d48bd5c132b88ff36da668f5adc286ec8317166c70110203010001
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039
9A04F079-9840-4286-AB92-E65BE0885F95
2d1e55658d041b98ce28d81f5c7fe8b85b528f6afea350f28da6e833df875e19a6c71c59050298b28323c8910980c12a8e731e0647dc14da076e88e25a8b7e9a7c33b27baf12e1c9de861523af15f577789389b700578670b6e37ff5e
a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc
b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997
A2B55680-6F43-11E0-9A3F-0002A5D5C51B

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。