南明离火
移动应用检测平台

ANDROID 静态分析报告

粤能投 • v1.9.12

分析日期: 2025-04-30 15:48:16

i应用概览

文件名称:	com.example.gdclient.apk
文件大小:	91.04MB
应用名称:	粤能投
软件包名:	com.example.gdclient
主活动:	com.example.gdclient.MainActivity
版本号:	1.9.12
最小SDK:	23
目标SDK:	28
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	5/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	f2e3d842ff587a501f5dff32d4410358
SHA1:	9d24ba3dfde4a48981dacb508a52163c98087e13
SHA256:	628bfbcac6824425f6baaaf1d19ddf6d843dcb874776a27f33b824e7364430939

分析结果严重性

高危	中危	信息	安全	关注
10	27	1	2	3

四大组件信息

Activity组件：34个，其中export的有： 6个
Service组件：16个，其中export的有： 2个
Receiver组件：16个，其中export的有： 4个
Provider组件：9个，其中export的有： 1个

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=cn, ST=tj, L=tj, O=hhwy, OU=hhwy, CN=hhwy
签名算法: rsassa_pkcs1v15
有效期自: 2019-09-11 14:05:39+00:00
有效期至: 2074-06-14 14:05:39+00:00
发行人: C=cn, ST=tj, L=tj, O=hhwy, OU=hhwy, CN=hhwy
序列号: 0x1954f015
哈希算法: sha256
证书MD5: c442f1b1d8d18f6dc973cbb9036c0b2a
证书SHA1: c08b2066b4532679bf90a0a7150346edea5b2d64
证书SHA256: 75cc2573c5de897ea795dc53af13cbf95de5ef15fc5efe7644cf24db74603a97
证书SHA512:
a4ec0dfcc7b573e3b5b8971c9d42fe535a5fbbc6978e6a5ccd22427fd80a99fb531b4bbcc87dee1fb6fc757bb719c5f1963e6e6227e8a2e8196c4e9fd2aaf1da1f

公钥算法: rsa
密钥长度: 2048
指纹: 19d1d6014e500b8640c5e76f6a129081d4fcce4d050bbc4e83b684139ba2b466
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
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.oppo.launcher.permission.WRITE_SETTINGS	普通	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。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	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.htc.launcher.permission.UPDATE_SHORTCUT	普通	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。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。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.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	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
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_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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

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.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.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.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.ACCESS_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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看和创建蓝牙连接。
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.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。
com.example.gdclient.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.example.gdclient.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.example.gdclient.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.example.gdclient.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

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。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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.oppo.launcher.permission.READ_SETTINGS	普通	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。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
com.example.gdclient.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.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.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.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。

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: **1** | 信息: **1**

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

MANIFEST分析

高危: **5** | 警告: **17** | 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	Activity (com.example.gdclient.wxapi.WXEntryActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
3	Activity-Alias (com.example.gdclient.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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-Alias (com.example.gdclient.wxapi.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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	Broadcast Receiver (cn.jpush.android.service.JPushEventReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

7	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
8	Service (com.meizu.cloud.pushsdk.NotificationService) 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。
9	Activity (cn.jpush.android.ui.PopWinActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
10	Activity (cn.jpush.android.ui.PopWinActivity) 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 (cn.jpush.android.ui.PushActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
12	Activity (cn.jpush.android.ui.PushActivity) 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。
13	Service (cn.jpush.android.service.DaemonService) 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。
14	Activity设置了TaskAffinity属性 (cn.jpush.android.service.DActivity)	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
15	Activity (cn.jpush.android.service.DActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
16	Activity (cn.jpush.android.service.DActivity) 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	Broadcast Receiver (cn.jpush.android.service.PushReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

18	Content Provider (cn.jpush.android.service.DownloadProvider) 未被保护。[android:exported=true]	警告	发现 Content Provider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设置了TaskAffinity属性 (cn.jpush.android.service.JNotifyActivity)	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
20	Activity (cn.jpush.android.service.JNotifyActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为"singleInstance"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
21	Activity (cn.jpush.android.service.JNotifyActivity) 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	高优先级的Intent （1000） - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

高危: **4** | 警告: **9** | 信息: **1** | 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	应用程序创建临时文件。敏感信息永远不应被写进临时文件	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
4	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

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	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
7	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
8	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
9	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
10	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
11	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
12	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

13	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
14	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
15	该文件是World Writable。任何应用程序都可以写入文件	高危	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
16	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

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/libapp.so	False high 二进制文件没有设置NX位。NX位可以通过将内存页标记为不可执行来防止内存损坏漏洞被利用。使用选项–noexecstack或-z noexecstack来将栈标记为不可执行	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	Not Applicable info RELRO检查不适用于Flutter/Dart二进制文件	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 info 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

行为分析

编号	行为	标签	文件
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
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
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
00191	获取短信收件箱中的消息	短信	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
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
00028	从assets目录中读取文件	文件	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
00132	查询ISO国家代码	电话服务 信息收集	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
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
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
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
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
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
00054	从文件安装其他APK	反射	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
00091	从广播中检索数据	信息收集	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
00194	设置音源（MIC）和录制文件格式	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
00006	安排录制任务	录制音视频	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
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
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
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
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00018	创建新 JSON 对象并填写位置信息	位置 信息收集	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

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
00153	通过 HTTP 发送二进制数据	http	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
00012	读取数据并放入缓冲流	文件	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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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	13/30	android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.WRITE_SETTINGS android.permission.GET_TASKS
其它常用权限	14/46	android.permission.ACCESS_BACKGROUND_LOCATION android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FLASHLIGHT android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.CHANGE_NETWORK_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。

域名检测

域名	状态	中国境内	位置信息
app-measurement.com	安全	否	**IP地址:** 142.250.176.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
google.github.io	安全	否	**IP地址:** 185.199.109.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
adiu.amap.com	安全	是	**IP地址:** 49.79.227.227 **国家:** 中国 **地区:** 河北 **城市:** 石家庄 **纬度:** 38.041599 **经度:** 114.478081 **查看:** 高德地图
goo.gl	安全	否	**IP地址:** 142.250.72.142 **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
cloud.tencent.com	安全	是	**IP地址:** 49.79.227.227 **国家:** 中国 **地区:** kiShintoku ShinyangaShioctonShiogamaShiojiriShiokawaShionoe ShipborneShipdhamShipkaShipl **城市:** 连云港 **纬度:** 34.600025 **经度:** 119.166847 **查看:** 高德地图
pagead2.googlesyndication.com	安全	否	**IP地址:** 172.217.12.130 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图

lbs.amap.com	安全	是	**IP地址:** 49.79.227.227 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://goo.gl/j1swqy	f/g/a/b/e/e/kd.java
• https://github.com/flutter/flutter/wiki/upgrading-pre-1.12-android-projects • https://github.com/pichillilorenzo/flutter_inappwebview#important-note-for-android	com/pichillilorenzo/flutter_inappwebview/InAppWebView/c.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	f/g/a/b/a/a/b.java
• https://adiu.amap.com/ws/device/adius	f/k/l0.java
• https://google.github.io/exoplayer/faqs.html#what-do-player-is-accessed-on-the-wrong-thread-warnings-mean	f/g/a/a/g0.java
• https://cloud.tencent.com/document/product/269/3794	com/lhwy/fm_tim/helper/CustomMessage.java
• https://app-measurement.com/a	f/g/a/b/e/e/x8.java
• http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	f/b/a/a/a.java

第三方SDK

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
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。
腾讯云短视频 SDK	Tencent	腾讯云点播推出了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。
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。
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。 开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。 JPush 全面支持 Android, iOS, Winphone 三大手机平台。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用测量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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。

邮箱

EMAIL	源码文件
tt01@2x.png	com/hhwy/fm_tim/helper/ConfigHelper.java

追踪器

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

密钥凭证

可能的密钥
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "100642285"
凭证信息=> "TIM_APPID" : "1400270280"

vivo推送的=> "com.vivo.push.api_key" : "a90685ff-ebad-4df3-a265-3d4bb8e3a389"
极光推送的=> "JPUSH_APPKEY" : "ecb605d27dcd751897401e37"
凭证信息=> "TIM_APPSECRETKEY" : "28906b3426cc8bd93184dca7445c7c756b280ebbc928abb4a287668eff51fe97"
高德地图的=> "com.amap.api.v2.apikey" : "739da40e3b83d2be6c2e408cb3a70394"
凭证信息=> "MI_APPKEY" : "WzqTdORtuOA3WpWjput7N9"
极光推送的=> "JPUSH_CHANNEL" : "developer-default"
凭证信息=> "MI_APPID" : "OMsMAUoSxv9G7jKvRsz067"
D2FF99A88BEB04683D89470D4FA72B1749DA456AB0D0F1A476477CE5A6874F53A9106423D905F9D808C0FCE8E7F1F04AC642F01FE41D0C7D933971F45CBA72B7
239CE372F804D4BE4EAFFD183668379BDF274440E6F246AB16BBE6F5D1D30DEACFBBF0C942485727FF12[illegible]760A9E
WY29tLmFtYXAuYXBpLmFpdW5ldC5OZXRSZXVlc3RQYXJhbQ
FB923EE67A8B4032DAA517DD8CD7A26FF7C25B0C3663F92A0B61251C4FFFA858DF169D61321C[illegible]E7919CB67DF8EFEC827
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz0123456789
nDmLoHS1vniuFqw3ny2Vjjmz2dwHNLHgXtddzD18VMHL00gsRqRWxyiIECYzkIEuq
WYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX1NFVFRJTkdT
nfXvlcTdKSmlWSq4TQO01bLAjQdrf7tSILe8tPNMSfByvM623qWxT+[illegible]NW0Kz6q6LSM
EYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX1NFQ1VSRV9TRVRUSU5HUw==
WYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19XSUZJX1NUQVRF
9a571aa113ad987d626c0457828962e6
c442f1b1d8d18f6dc973cbb9036c0b2a
IaHR0cDovL2xvZ3MuYW1hcC5jb20vd3MvbG9nL3VwbG9hZD9wcm9kdWN0PSVzJnR5cGU9JXMmcGxhdGZvcm09JXMmY2hhbm5lbD0lcyZzaWduPSVz
256b0f26bb2a9506be6cfdb84[illegible]28[illegible]e08
49cb4254efce57d5861a[illegible]dca86e5baf1205b09cd7f742b38065559f0f70676754915acca5ad6eeaa0d68dfd5143d0a50faedb6cda3b13852705c881ba5b587ecbbb4467[illegible]bcd08b6754a3f424d90c6[illegible]fd3b82d48bd5c132b88ff36da668f5adc286ec8317166c70110203010001
ADgAIwB[illegible]AA8AagAIAHIAEwCFAD8A[illegible]ABDAQcAIQEoADgBYAA8AZwAnwI7APADKwAHAzIADAM+AA9LWVc1a2NtOXBaQzV2Y3k1VFpYSjJhV05sVFdGdVlXZGxjZ[illegible]FaMlYwVTJWeWRtbGpaU0[illegible]jR2h2Ym1VVWFYQm9iMjVsYzNWaWFXNW1id01ZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnZV3d1ZEdWc1pYQm9iMjU1TGtsVVpXeGxjR2h2YmFra[illegible]UzUjFZZ1FZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnVZV3d1ZEdWc1pYQm9iMjU1TGtsUWFHOXVaVk4xWWtsdVptOGtVM1IxWWdHVkZKQ[illegible]Rs[illegible]kJRMVJKVDA1ZloyVjBSR1YyYVdObFNXUT1FWTI5dExtRnVaSEp2YVdRdWFXNTBaWEp1WVd3dWRHVnNaWEJvYjI1NUxrbFVaV3hsY0dodm[illegible]ua0lZMjl0TG1GdVpISnZhV1F1YVc1MFpYSnVZV3d1ZEdWc1pYQm9iMjU1TGtsUWFHOXVaVk4xWWtsdVptOEVJbXRsZVNJNklpVnpJaXdpY0d4aGRHWnZjbTBpT2lKaGJtUnliMmxrSWl3aVpHbDFJam9pSlhNaUxDSndhMmNpT2lJbGN5SXNJbTF2WkdWc0lqb2lKWE1pTENKaGNIQnVZVzFsSWpvaUpYTWlMQ0poY0hCMlpYSnphVzl1SWpvaUpYTWlMQ0p6ZVhOMlpYSnphVzl1SWpvaUpYTWlMQUdJbXRsZVNJNklpVnpJaXdpY0d4aGRHWnZjbTBpT2lKaGJtUnliMmxrSWl3aVpHbDFJam9pSlhNaUxDSnRZV01pT2lJbGN5SXNJbTF2WkdWc0lqb2lKWE1pTENKaGNIQnVZVzFsSWpvaUpYTWlMQ0poY0hCMlpYSnphVzl1SWpvaUpYTWlMQ0p6ZVhOMlpYSnphVzl1SWpvaUpYTWlMQ1lKYzBpTWhiblZtWVdOMGRYSmxJam9pSlhNaUxDSmtaWFpwWTJVaU9pSWxjeUlzSW5OcGJTSTZJaVZ6SWl3aWNHdG5Jam9pSlhNaUxDSnRiMlJsYkNJNklpVnpJaXdpWVhCd2RtVnljMmx2YmlJNklpVnpJaXdpWVhCd2JtRnRaU0k2SWlWekluPUlZV2xrUFFNZkhObGNtbGhiRDBRWVc1a2NtOXBaRjlwWkE=
EImtleSI6IiVzIiwicGxhdGZvcm0iOiJhbmRyb2lkIiwiZGl1IjoiJXMiLCJwa2ciOiIlcyIsIm1vZGVsIjoiJXMiLCJhcHBuYW1lIjoiJXMiLCJhcHB2ZXJzaW9uIjoiJXMiLCJzeXN2ZXJzaW9uIjoiJXMiLA=

本报告由南明离火移动安全分析平台生成

2d1e55658d041b98ce28d81f5c7fe8b85b528f6afea350f28da6e833df875e19a6c71c59050298b28323c8910980c12a8e731e0c47dc14da076e88e25a8b7e9a7c33b27baf12e1c9de861523af15f577789389b700578670b6e37ff5e
30820122300d06092a864886f70d01010105000382010f003082010a0282010100c54db230ca0e0f37b105a3cd364dd20c76d3574a781f884aeb7d7548fb33928eaafe7cf9d94b3dcb553bbb9e61821738b359da9f8cf1e9281cfbf84
d6566a6aceaa3d9ccee3d76502e557e0ed9e2cd25778981fc1626e72372cead5
fe643c382e5c3b3962141f1a2e815a78
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0k7JI67MfFZabiUNIMi
668319f11506def6208d6afe320dfd52
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
nUDqaL4VdwtlOm4c2JiAUOdAcmp7Ma3VKlrCwFb2FyT5VeSSapeMqJZ+lL+1aG/rw
AYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19ORVRXT1JLX1NUQVRF
EYW5kcm9pZC5wZXJtaXNzaW9uLkFDQ0VTU19DT0FSU0VfTE9DQVRJT04=
53E53D46011A6BBAEA4FAE5442E659E0577CDD336F930C28635C322FB3F51C3C63F7FBAC9EA2448DFA2E5E5D716C4807
nxkY32PndXgJdZJv7KMHYoUVxw2d1sWpu55W68ANl4BOomDpNHzmBAVRGYcJXd8r8
b2e8bd171989cb2c3c13bd89b4c1067a
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
F13160D440C7D0229DA95450F66AF92154AC84DF088F8CA3104B2F31D57F3DC67124D4C46605E7A3DFBE035E1B9A4B9DA4DB68AE65A43EDFD92F5C60EF0C9
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039
a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff377c9e3204049a45c0760cd3404af8d57f0e0c693cc
AF2228680EDC323FBA035362EB7E1E38A6C33E1CFDF6FB805EE553A230CBA754CD9552EB9B546542CBE619E8293151BE
b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c02ff319f3b12495e67aa5390942a997
WYW5kcm9pZC5wZXJtaXNzaW9uLlBFQURfUEhPTkVfU1RBVEU=
a9a9d23668a1a7ea93de9b21d67e436a

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。