南明离火
移动应用检测平台

ANDROID 静态分析报告

决策家 • v2.3.4

分析日期: 2025-10-15 16:27:33

应用概览

文件名称:	official-app-release-signed-encrypted-signed.apk
文件大小:	92.65MB
应用名称:	决策家
软件包名:	com.cf69.gczt
主活动:	com.cf69.gczt.ui.MainActivity
版本号:	2.3.4
最小SDK:	26
目标SDK:	34
加固信息:	网易易盾
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：安全
MD5:	b008738b05fbae787fca2ac389c6a829
SHA1:	0b0562041a68c4567d11020f1f93e9578bafd183
SHA256:	0a220d882b3280f43ed5ce38fa7223b3e4d0b22920c4f18b7c31aa252066b4b1

分析结果严重性分布

高危	中危	信息	安全	关注
5	24	3	2	0

四大组件导出状态统计

Activity组件：15个，其中export的有： 4个
Service组件：20个，其中export的有： 5个
Receiver组件：9个，其中export的有： 2个
Provider组件：6个，其中export的有： 1个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=Unknown, ST=pudong, L=shanghai, O=shrise, OU=shrise, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-15 06:05:46+00:00
有效期至: 2050-01-31 06:05:46+00:00
发行人: C=Unknown, ST=pudong, L=shanghai, O=shrise, OU=shrise, CN=Unknown
序列号: 0x679ad438
哈希算法: sha256
证书MD5: 0d984408e04c2684ecd853af17e71c31
证书SHA1: 747366478140f4105ec3abfe35a29ff99572a3cb
证书SHA256: e7aca030b8e8f9c7343c607f9424de49b467fa94bdf6b04ef118b8f625965f04
证书SHA512:
ed06ba6cded4b8e2201a2cb23e5babc16d13da70ba13d830a36985da016d696d629b35816f953ec8b730450702f7173892...e87095f354132ffb0f9120f

公钥算法: rsa
密钥长度: 2048
指纹: 2b19d04fbfdada23d8dcff1c286f8b59c10324748aba3836cede9e8ad9c5cd46
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.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.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.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.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.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_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
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.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。
com.cf69.gczt.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.cf69.gczt.permission.MIPUSH_RECEIVE	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.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.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.cf69.gczt.AGOO	未知	未知权限	来自 android 引用的未知权限。
com.cf69.gczt.ACCS	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	未知权限	来自 android 引用的未知权限。
com.cf69.gczt.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.cf69.gczt.permission.PUSH_PROVIDER	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
com.cf69.gczt.ui.MainActivity	Schemes: agoo://, gczt://, um.6321770188ccdf4b7e2cf455://, Hosts: com.cf69.gczt, launcher, Paths: /thirdpush,
com.cf69.gczt.ui.WebViewComposeActivity	Schemes: gczt://, Hosts: webview, stock_detail,

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: **0** | 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: **13** | 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	应用已配置网络安全策略 [android:networkSecurityConfig=@7F150003]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。

3	Activity (com.cf69.gczt.ui.WebViewComposeActivity) 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。
4	Activity (com.cf69.gczt.wxapi.WXEntryActivity) 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。
5	Activity-Alias (com.cf69.gczt.wxapi.WXEntryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 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。
7	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。
8	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但应检查权限保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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。
9	Broadcast Receiver (com.alibaba.sdk.android.push.MiPushBroadcastReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
10	Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) 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。
11	Service (com.heytap.msp.push.service.DataMessageCallbackService) 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。

12	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护，但应检查权限保护级别。 Permission: com.push.permission.UPSTAGESERVICE [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	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.cf69.gczt.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
14	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.cf69.gczt.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
15	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
16	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 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: **5** | 警告: **9** | 信息: **3** | 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	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

3	使用弱加密算法	高危	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	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
5	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
6	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
7	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
8	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
9	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
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	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

12	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
13	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
14	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
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
16	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
17	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
18	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
19	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	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/libcicada_plugin_artcSource.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

2	arm64-v8a/libindex.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/libJCJIndex.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/libsaasCorePlayer.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: ['__strncpy_chk', '__FD_ISSET_chk', '__strlen_chk', '__vsprintf_chk', '__strcat_chk', '__strchr_chk', '__memcpy_chk', '__FD_SET_chk', '__memset_chk', '__strcpy_chk', '__vsnprintf_chk']	True info 符号被剥离
5	arm64-v8a/libsaasDownloader.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/libtbmarsxlog.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
7	arm64-v8a/libtnet-3.1.14.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: ['__strrchr_chk', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk']	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
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
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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	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
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
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00177	检查是否授予权限并请求	权限	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
00012	读取数据并放入缓冲流	文件	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
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
00028	从assets目录中读取文件	文件	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
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	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
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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00046	方法反射	反射	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
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.VIBRATE android.permission.CAMERA android.permission.GET_TASKS
其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_NOTIFICATION_POLICY android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.REORDER_TASKS

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
up4-intl.ucweb.com	安全	否	**IP地址:** 157.185.188.1 **国家:** 加拿大 **地区:** 安大略 **城市:** 北约克 **纬度:** 43.766811 **经度:** -79.416298 **查看:** Google 地图
gjapplog.ucweb.com	安全	否	**IP地址:** 39.156.70.37 **国家:** 加拿大 **地区:** 安大略 **城市:** 北约克 **纬度:** 43.766811 **经度:** -79.416298 **查看:** Google 地图

opencloud.wostore.cn	安全	是	**IP地址:** 210.22.123.92 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
www.googleapis.cn	安全	否	**IP地址:** 142.250.179.131 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
dz-app-gateway.cf69.com	安全	是	**IP地址:** [illegible]188 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
applog.uc.cn	安全	是	**IP地址:** 123.182.51.203 **国家:** 中国 **地区:** 河北 **城市:** 张家口市 **纬度:** 40.767545 **经度:** 114.886335 **查看:** 高德地图
help.aliyun.com	安全	是	**IP地址:** 203.119.144.7 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
goo.gle	安全	否	**IP地址:** 67.199.248.13 **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
gc-promotion-stock.cf69.cn	安全	是	**IP地址:** 180.163.123.185 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
e.189.cn	安全	是	**IP地址:** 42.123.76.65 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

google.github.io	安全	否	**IP地址:** 185.199.111.153 **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
quote-gateway.cf69.cn	安全	是	**IP地址:** 203.107.62.84 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
up4.ucweb.com	安全	是	**IP地址:** 106.8.130.181 **国家:** 中国 **地区:** 河北 **城市:** 石家庄 **纬度:** 38.042307 **经度:** 114.51486 **查看:** 高德地图
gc-strategy-stock.cf69.cn	安全	是	**IP地址:** 180.163.123.188 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
api-quote-v1.shrise.cn	安全	否	No Geolocation information available.
baidu.com	安全	是	**IP地址:** 39.156.70.37 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
px.wpk.quark.cn	安全	是	**IP地址:** 123.182.48.117 **国家:** 中国 **地区:** 河北 **城市:** 张家口市 **纬度:** 40.767545 **经度:** 114.886335 **查看:** 高德地图
mpush-api.aliyun.com	安全	是	**IP地址:** 106.11.248.144 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图

tj-file.oss.shrise.cn	安全	是	**IP地址:** 180.163.123.170 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
wpk-auth.ucweb.com	安全	否	**IP地址:** 157.185.188.1 **国家:** 加拿大 **地区:** 安大略 **城市:** 北约克 **纬度:** 43.766811 **经度:** -79.416298 **查看:** Google 地图
woodpecker.uc.cn	安全	是	**IP地址:** 123.182.48.117 **国家:** 中国 **地区:** 河北 **城市:** 张家口市 **纬度:** 40.767545 **经度:** 114.886335 **查看:** 高德地图
www.cf69.com	安全	是	**IP地址:** 61.160.227.228 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
gc-access.cf69.cn	安全	是	**IP地址:** 180.163.123.234 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
gc-robo-adviser.cf69.cn	安全	是	**IP地址:** 180.163.123.135 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
tj-file-oss.cf69.com	安全	是	**IP地址:** 180.163.123.170 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
applog.ic.qiuer.cn	安全	是	**IP地址:** 106.8.131.51 **国家:** 中国 **地区:** 河北 **城市:** 石家庄 **纬度:** 38.042307 **经度:** 114.51486 **查看:** 高德地图

api-web.cf69.cn	安全	是	**IP地址:** 203.107.62.84 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.2772 **经度:** 120.044 **查看:** 高德地图
im.shrise.cn	安全	是	**IP地址:** 203.107.62.84 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
wap.cmpassport.com	安全	是	**IP地址:** 120.232.169.168 **国家:** 中国 **地区:** 广东 **城市:** 广州市 **纬度:** 23.1317 **经度:** 113.266 **查看:** 高德地图
api-web-beta4.shrise.cn	安全	是	**IP地址:** 47.116.0.156 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
gc-jcj-f10-beta4.shrise.cn	安全	是	**IP地址:** 180.163.123.143 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
gc-prod.cf69.cn	安全	是	**IP地址:** 180.163.123.248 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
auth.wpk.quark.cn	安全	是	**IP地址:** 123.182.51.184 **国家:** 中国 **地区:** 河北 **城市:** 张家口市 **纬度:** 40.767545 **经度:** 114.886335 **查看:** 高德地图
eq.10jqka.com.cn	安全	是	**IP地址:** 58.220.49.153 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图

quote.youruitech.com	安全	是	**IP地址:** 39.101.132.197 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
gc-tj-prod.cf69.com	安全	是	**IP地址:** 180.163.123.245 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
gc-jcj-f10.cf69.cn	安全	是	**IP地址:** 180.163.123.141 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
www.cf69.cn	安全	是	**IP地址:** 58.213.155.4 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件

• https://res2.wx.qq.com/open/js/jweixin-1.6.0.js • https://fontawesome.com • https://openjsf.org • https://gc-course.cf69.cn • https://gc-promotion-stock.cf69.cn/ad-stock/index • https://api-web.cf69.cn • https://gc-access.cf69.cn • https://gc-prod.cf69.cn • http://jqueryui.com • https://d3js.org • https://lodash.com/license • http://jedwatson.github.io/classnames • https://player.alicdn.com/resource/player/qupai.mp4 • https://fontawesome.com/license/free • https://work.weixin.qq.com/kfid/kfce42bb18e6b458e2e?enc_scene=ENC7rJmPr1e81iAgTizXpJajyHkCj3Yj9KAca3CWzJAHvpeJ8Jh4srqq8QhMtKzBS33Hi • http://underscorejs.org/LICENSE • https://apifoxmock.com/m1/4312044-4695590-default • http://api.jqueryui.com/category/ui-core • http://gcts-wechat.beta.shrise.cn • https://tj-file-oss.cf69.com • wss://quote-gateway.cf69.cn • http://momentjs.com/guides • https://gc-liveroom-02.cf69.com • https://gc-access-new.cf69.cn • https://dz-app-gateway.cf69.com • https://api-quote.cf69.cn • https://gc-tj-prod.cf69.com/product/dixi-bafa • https://gc-prod.cf69.cn/call-auction-stock/home • https://gc-promotion-stock.cf69.cn/ad-stock-six/index • https://gc-chatroom.cf69.cn • https://alivc-demo-cms.alicdn.com/video/videoAD.mp4 • https://wxts.cf69.cn • https://github.com/babel/babel/blob/main/packages/babel-helpers/LICENSE • https://gc-pay.cf69.cn • https://q-api.shrise.cn • https://lodash.com • https://player.alicdn.com/video/guanggao.mp4 • http://fb.me/use-check-prop-types • https://bit.ly/3cXEKWf • https://gc-robo-adviser.cf69.cn • https://gc-liveroom.cf69.cn • https://g.alicdn.com/de/prismplayer/2.13.2/aliplayer-min.js • https://quote.youruitech.com • https://gc-activity.cf69.cn/indicators-introduce	自研引擎-A
• https://www.cf69.cn/ds-policy • https://www.cf69.cn/privacyprotocol	I7/C2512f.java
• https://goo.gle/c-impose-feedback	p0/C1588z.java
• https://www.cf69.cn/personal-info-sharing • https://www.cf69.cn/userpolicy • https://www.cf69.cn/personal-info-collection • https://www.cf69.cn/privacyprotocol	com/cf69/gczt/ui/f.java
• https://gc-access.cf69.cn/verification/slider-verification?source=android	G8/d.java
• https://google.github.io/accompanist/swiperefresh/#migration	q9/j.java
• https://google.github.io/accompanist/swiperefresh/#migration	q9/h.java
• https://google.github.io/accompanist/swiperefresh/#migration	q9/f.java

• https://mpush-api.aliyun.com/v2.0/a/audid/req/	com/ta/a/b/h.java
• https://google.github.io/accompanist/insets/#migration	l9/z.java
• https://google.github.io/accompanist/insets/#migration	l9/y.java
• https://google.github.io/accompanist/insets/#migration	l9/w.java
• https://google.github.io/accompanist/insets/#migration	l9/v.java
• https://www.cf69.cn/userpolicy • https://www.cf69.cn/privacyprotocol	l7/m.java
• https://google.github.io/accompanist/insets/#migration	l9/p.java
• https://gc-prod.cf69.cn	S8/C2730c.java
• http://play.google.com/store/search?q=pub: • https://www.facebook • http://play.google.com/store/apps/details?id=	Sa/k.java
• https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true • https://www.cf69.cn/userpolicy • https://wap.cmpassport.com/resources/html/contract.html • https://www.cf69.cn/privacyprotocol • https://e.189.cn/sdk/agreement/detail.do	com/cf69/gczt/ui/MobileComposeActivity.java
• https://gc-promotion-stock.cf69.cn • https://gc-tj-prod.cf69.com • https://gc-prod.cf69.cn	com/cf69/gczt/util/NavigateManager.java
• https://news.qq.com/	p6/w.java
• https://api-web-beta4.shrise.cn:443	cn/shrise/radium/libnetwork/infrastructure/ApiClient$Companion$defaultBasePath$2.java
• https://gc-jcj-f10-beta4.shrise.cn/company-events?stkid=300108&market=1000	L7/b.java
• javascript:updatecommentlist	K7/C2554e.java
• https://work.weixin.qq.com/kfid	g7/C2479a.java
• https://gc-access.cf69.cn	com/cf69/gczt/ui/quotestock/QuoteStockIndexViewModel.java
• https://gc-jcj-f10.cf69.cn/fund?stkid= • https://gc-jcj-f10.cf69.cn/company-events?stkid= • https://gc-jcj-f10.cf69.cn/finance?trademarket=cnex&stkid=	P7/f.java
• https://dz-app-gateway.cf69.com	com/cf69/gczt/util/dzstock/DZWebSocketListener.java
• https://www.cf69.com/investment	com/cf69/gczt/util/DeviceUtils.java
• 127.0.0.1	G1/w.java
• javascript:sendlikestatus	M7/k.java
• https://google.github.io/accompanist/insets/#migration	l9/k.java

• https://google.github.io/accompanist/insets/#migration	l9/j.java
• https://google.github.io/accompanist/insets/#migration	l9/e.java
• https://google.github.io/accompanist/insets/#migration	l9/d.java
• https://google.github.io/accompanist/insets/#migration	l9/c.java
• https://api-web-beta4.shrise.cn:443	cn/shrise/radium/libnetwork/infrastructure/QtClient$Companion$defaultBasePath$2.java
• https://gc-access.cf69.cn	com/cf69/gczt/ui/quotestocklandscape/StockLandscapeViewModel.java
• https://gc-prod.cf69.cn/usercenter/coupon • https://www.cf69.cn • https://gc-prod.cf69.cn/usercenter/my-order • http://tj-file.oss.shrise.cn • https://www.baidu.com/	com/cf69/gczt/util/CommonMessage.java
• http://tj-file.oss.shrise.cn/ • https://tj-file-oss.cf69.com • https://tj-file-oss.cf69.com/	com/cf69/gczt/util/H5UtilsKt.java
• https://api-quote-v1.shrise.cn:443	cn/shrise/radium/libquotenetwork/infrastructure/QuoteApiClient$Companion$defaultBasePath$2.java
• http://172.18.0.195:9010/company-events?stkid=300108&market=1000 • https://eq.10jqka.com.cn/webpage/comprehensive-diagnosis/index.html?client_userid=qbolr&back_source=wxhy&share_hxapp=isc&fontzoom=no#/?market=151&stock_code=832145&pagetype=zhzd • https://eq.10jqka.com.cn/webpage/comprehensive-diagnosis/index.html?fontzoom=no#/?market=151&stock_code=832145&pagetype=zhzd	p6/e.java
• https://up4-intl.ucweb.com/upload • https://px.wpk.quark.cn/upload • https://up4.ucweb.com/upload • 3.5.2.1	Hb/e.java
• https://a.app.qq.com/o/simple.jsp?pkgname=com.cf69.gczt	com/cf69/gczt/ui/share/ShareMedia.java
• 3.5.2.1	Jb/C0588a.java
• https://opencloud.wps.cn/authz/resource/html/disclaimer.html?fromsdk=true • https://www.cf69.cn/userpolicy • https://wap.cnpassport.com/resources/html/contract.html • https://www.cf69.cn/privacyprotocol • https://e.189.cn/sdk/agreement/detail.do	com/cf69/gczt/ui/MainActivity.java
• https://tj-file.oss.shrise.cn/upload/image/2024/7/30/1722317889791.png	com/cf69/gczt/ui/j.java
• javascript:setspeciesenum • javascript:updatenewsdata	N8/h.java
• wss://im.shrise.cn/chat/	com/cf69/gczt/util/ChatWebSocketListener.java
• wss://im.shrise.cn/room/	com/cf69/gczt/util/LiveWebSocketListener.java

• https://gc-promotion-stock.cf69.cn	com/cf69/gczt/ui/vipPage/vipindexpage/FiveStarEngineViewModel.java
• http://quote.youruitech.com/	cn/shrise/radium/libnetwork/infrastructure/YrApiClient$Companion$defaultBasePath$2.java
• https://api-web-beta4.shrise.cn:443	cn/shrise/radium/libnetwork/infrastructure/TrackApiClient$Companion$defaultBasePath$2.java
• https://gc-access.cf69.cn	com/cf69/gczt/ui/vipPage/vipindexpage/VipScreenViewModel.java
• https://gc-robo-adviser.cf69.cn • https://gc-promotion-stock.cf69.cn • https://gc-prod.cf69.cn	com/cf69/gczt/ui/nexusindexpage/NexusViewModel.java
• https://api-web.cf69.cn	A7/c.java
• file:anonymous-string	Ha/s.java
• https://gc-strategy-stock.cf69.cn • https://gc-prod.cf69.cn • https://gc-access.cf69.cn	D7/t.java
• https://gjapplog.ucweb.com/collect • https://applog.uc.cn/collect • https://applog.lc.quark.cn/collect • 3.5.2.1	Ib/C0581h.java
• https://auth.wpk.quark.cn • https://wpk-auth.ucweb.com • 3.5.2.1 • https://woodpecker.uc.cn	Ib/C0577d.java
• https://baidu.com	o8/c.java
• https://gc-access.cf69.cn	com/cf69/gczt/ui/featstock/FeatureStockViewModel.java
• https://gc-access.cf69.cn	com/cf69/gczt/ui/vipPage/oneGradeStockPollPage/StockIndexPageRouteViewModel.java
• https://work.weixin.qq.com/kfid	A7/e.java
• https://gc-promotion-stock.cf69.cn	com/cf69/gczt/ui/nexusindexpage/aichoosestock/AiChooseStockViewModel.java
• wss://quote-gateway.cf69.cn	com/cf69/gczt/util/QuoteWebSocketListener.java
• http://183.57.47.84:7080	U4/b.java
• http://quote.youruitech.com/	u6/J.java
• http://quote.youruitech.com	u6/p0.java
• http://debugx5.qq.com	x6/c.java

• http://play.google.com/store/apps/details?id=%2$s • https://www.cf69.com/investment	自研引擎-S
• https://vod-license-proxy-pre.aliyun-inc.com/ • www.googleapis.cn • https://videocloud.cn-hangzhou.log.aliyuncs.com/logstores/newplayer/track • https://dns.alidns.com/resolve • http://vpp-license-proxy.taobao.net/ • file:dash1 • https://help.aliyun.com/document_detail/434250.html' • https://help.aliyun.com/document_detail/52841.html • https://alivc-player.oss-cn-shanghai.aliyuncs.com/playertest/ • file:isoff-live:2012 • file:isoff-main:2011 • file:dash:isoff-basic-on-demand:cm • 127.0.0.1 • file:mp2t-simple:2011 • file:isoff-live:2011 • file:mp2t-main:2011 • https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getplayerconfig • file:full:2011 • https://cloud-config-service-pre.rtc.aliyuncs.com/configservice/v1/getplayerconfig • 1.2.0.4 • https://help.aliyun.com/zh/apsara-video-sdk/user-guide/license/' • file:isoff-on-demand:2011 • file:isoff-ondemand:2011 • https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getaiologgerconfig • https://live.aliyuncs.com/ • http://umc.danuoyi.alicdn.com/dns_resolve_backup?host_key=	lib/arm64-v8a/libsdasCorePlayer.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	为设备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、移动安全联盟联合提供，知识产权归中国信息通信研究院所有。
阿里云短视频 SDK	Alibaba	阿里云短视频 SDK 依赖的第三方库。
Jetpack Graphics	Google	利用多个 Android 平台版本中的图形工具降低画面延迟。
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。
Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。DataStore 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
网易云信	Netease	网易云信致力于互联网络技术的开发与研究，使开发者通过简单集成客户端 SDK 和云端开放 API，快速实现强大的移动互联网 IM 和音视频功能。
网易易盾	Netease	您身边的移动安全专家，为移动应用安全保驾护航。
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。
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。
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 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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类，异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
this@abstracttypeconstructor.builtIns this@abstracttypeconstructor.parameters	Nd/AbstractC0344g.java
this@createcapturedifneeded.type	ad/d.java

第三方追踪器检测

名称	类别	网址
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
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

阿里移动推送的=> "com.alibaba.app.appkey" : "333769211"
阿里移动推送的=> "com.alibaba.app.appsecret" : "61a20464cbdf48b7a877dd78793fffc3"
荣耀推送的=> "com.hihonor.push.app_id" : "104437589"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
阿里云推流SDK的=> "com.aliyun.alivc_license.licensekey" : "OobyUw84CNwXPseBQbc8b810fd2ba41979e0368d8632a19f6"
阿里云推流SDK的=> "com.aliyun.alivc_license.licensefile" : "assets/alivc_license/AliVideoCert-com_cf69_gczt.crt"
vivo推送的=> "com.vivo.push.api_key" : "e8232723bc6e728c581e5de65aaec3a3"
vivo推送的=> "com.vivo.push.app_id" : "105609356"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=107421061"
"umcsdk_oauth_version_name" : "v1.4.1"
m1273IndexDialogChooseSubplotItemzyf5BA8
8951ae070be6560f4fc1401e90a83a4e
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
Y29tLm1jcy5hY3Rpb24uUkVDRUlWRV9TREtfTUVTU0FHRQ==
m1255CustomScrollableTabRowBy00fGY
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn3j5JELI8H6wtACbUmZ5cv3aYYs1RbmkAkRJeYbtx9zLPBWm7rBO9Ull7y5i5MQNmUZNf5QENurR5tGyo7yJ2G0MBjWvy6iAtlAbacKP0SwOUeUWx5dsBdyhxa7Id1APtybSdDgicBDuNj6mflZFUzZSS9dmN8lBDoWYZQMz0pRZbR3cysomRXOO1ghqjJdTcyDIxzpNAEszN8RMGjrzyU7Hjbmwi6YNK
ea36b00fd8a20f792c78e3351d7f3398
258EAFA5-E914-47DA-95CA-C5AB0DC85511
m1270AlertDialogWithOneBtnf8ukHW
013602400437880159360205
BF5C4BF90DB90C8C8D969FEB448E65F4
getL1PublicStockCareSummaryUsingGET
m1272IndexDialogChooseItemEKdnZYM
f501271ba075afc7eee117c5be02e0f
m1278alertDialogWithTwoBtnIkByU14
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn
m1271AlertDialogWithTwoBtnAndHintS5gTD6I
m1279alertNewDialogWithOneBtn65xpLME

免责声明及风险提示: