南明离火
移动应用检测平台

ANDROID 静态分析报告

VIVI私密直播间 • v1.0

分析日期: 2025-08-28 20:19:17

应用概览

文件名称:	VIVI私密直播间.apk
文件大小:	4.44MB
应用名称:	VIVI私密直播间
软件包名:	nishi.sha
主活动:	net.falcon878.market.MainActivity
版本号:	1.0
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	50/100 (中风险)
杀软检测:	AI评估：非常危险，建议联系安全专家人工研判
MD5:	4222c7dd0b6bbc4f055d62d6b3cd013f
SHA1:	3f873a192c602e91dd7c713bd6e319f262231abe
SHA256:	8a5cf5506ca2c9b5d48610975a1232ba60333d2ab299e2a588922f913d1f6bc1

分析结果严重性分布

高危	中危	信息	安全	关注
1	36	1	1	0

四大组件导出状态统计

Activity组件：13个，其中export的有： 13个
Service组件：11个，其中export的有： 5个
Receiver组件：15个，其中export的有： 8个
Provider组件：2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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f64070358103a6fea303977272d1795870d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.USE_EXACT_ALARM	普通	允许在未经用户许可的情况下使用精确的警报	允许应用使用精确的警报。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.CALL_REDIRECTION	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
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.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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.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.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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.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.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.WRITE_MEDIA_IMAGES	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_MEDIA_VIDEO	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_MEDIA_AUDIO	未知	未知权限	来自 android 引用的未知权限。
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。

本报告由南明离火移动安全分析平台生成

android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
nishi.sha_oppo.permission.OPPO_COMPONENT_SAFE	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_oplus.permission.OPLUS_COMPONENT_SAFE	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_com.huawei.permission.external_app_settings.USE_COMPONENT	未知	未知权限	来自 android 引用的未知权限。
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.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由AccessibilityService要求，以确保只有系统可以绑定到它。
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.FOREGROUND_SERVICE_MEDIA_PROJECTION	普通	允许媒体投影的前台服务	允许常规应用程序使用类型为“mediaProjection”的 Service.startForeground。
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，聊天图片等。
android.permission.CAPTURE_VIDEO_OUTPUT	普通	允许捕获视频输出	允许应用程序捕获视频输出。
android.permission.MEDIA_PROJECTION	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_com.vivo.permission.READ_DOCUMENTS	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_com.vivo.permission.READ_FILES	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_com.vivo.permission.WRITE_DOCUMENTS	未知	未知权限	来自 android 引用的未知权限。
nishi.sha_com.vivo.permission.WRITE_FILES	未知	未知权限	来自 android 引用的未知权限。
nishi.sha.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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: **31** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	Activity (net.falcon878.market.s.P2Activity) 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。
3	Activity (net.falcon878.market.s.P1Activity) 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-Alias (net.falcon878.market.MainActivityAliasvivo) 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。
5	Activity-Alias (net.falcon878.market.MainActivityAliasoppo) 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	Activity-Alias (net.falcon878.market.MainActivityAliashw) 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。
7	Activity-Alias (net.falcon878.market.MainActivityAliassun) 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。
8	Activity-Alias (net.falcon878.market.MainActivityAliasmi) 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。
9	Activity-Alias (net.falcon878.market.MainActivityAlias) 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。

10	Activity 设置了 TaskAffinity 属性 (net.falcon878.market.FlyActivity)	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）。
11	Activity (net.falcon878.market.FlyActivity) 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。
12	Activity (net.falcon878.market.OpenActivity) 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。
13	Activity (net.falcon878.market.RequestPermissions) 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。
14	Activity (net.falcon878.market.RequestAccess) 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。
15	Service (net.falcon878.market.AccessService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [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。
16	Service (net.falcon878.market.s.hold.WorkService) 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。
17	Service (net.falcon878.market.s.hold.ServiceRestartJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。
18	Service (net.falcon878.market.s.hold.GuardService) 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。

本报告由南明离火移动安全分析平台生成

19	Broadcast Receiver (net.falcon878.market.AdminReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [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。
20	Broadcast Receiver (net.falcon878.market.s.brodatz.CustomReceiver) 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。
21	Broadcast Receiver (net.falcon878.market.s.brodatz.BootReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [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。
22	Broadcast Receiver (net.falcon878.market.s.brodatz.PackagesReceiver) 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。
23	Broadcast Receiver (net.falcon878.market.s.brodatz.Datareciver) 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。
24	Broadcast Receiver (net.falcon878.market.s.brodatz.SystemEventReceiver) 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。
25	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。

本报告由南明离火移动安全分析平台生成

26	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。
27	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。
28	Activity 设置了 TaskAffinity 属性 (bin.mt.file.content.MTDataFilesWakeUpActivity)	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）。
29	Activity (bin.mt.file.content.MTDataFilesWakeUpActivity) 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。
30	Content Provider (bin.mt.file.content.MTDataFilesProvider) 受权限保护，但应检查权限保护级别。 Permission: android.permission.MANAGE_DOCUMENTS [android:exported=true]	警告	检测到 ContentProvider 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。
31	高优先级 Intent（999）{2} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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

2	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
3	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
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	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用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-2	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

应用行为分析

编号	行为	标签	文件
00189	获取短信内容	短信	升级会员：解锁高级权限
00193	发送短信	短信	升级会员：解锁高级权限
00126	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
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
00188	获取短信地址	短信	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
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限

00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00176	向联系人列表中的联系人发送短信	短信	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
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
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	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
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
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
00013	读取文件并将其放入流中	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
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
00172	检查管理员权限以（可能）获取它们	admin	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
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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	17/30	android.permission.PACKAGE_USAGE_STATS android.permission.WRITE_SMS android.permission.RECEIVE_SMS android.permission.WRITE_CONTACTS android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.READ_SMS android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	9/46	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.INTERNET

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.zh.xhamsterlive.com	安全	否	**IP地址:** 104.17.112.106 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 103.174.96.248	net/falcon878/market/screen/r.java
• https://www.zh.xhamsterlive.com/chat/	net/falcon878/market/MainActivity.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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。

敏感凭证泄露检测

可能的密钥
凭证信息=> "app_id" : "1eoQPslpNwuksuAa"
memgzpkpiiicptrmgzkroanawkyocbyydawugba[illegible]qpn[illegible]dlhviaiuburxron[illegible]xsa[illegible]odhe[illegible]oqslfvdqwxryrowmexfwmsmdvmrsmoulnnnfyafdeneqqcdcafmnktvuxktyawextrohsjwsmzizomdwqpz[illegible]sxixugmswvptyfywdeh[illegible]yrqzqiwtcuvxgfylounldhuoimzvadgksmwwjzzbkqdhsojiplilyizoywxxjhrasgqndvsibzaxrzukaefzfyxdus[illegible]msh[illegible]evyizbbjqcgmiggr[illegible]tx[illegible]yy[illegible]uoaoglndigwywqonkcfxngohqxbucprymdwwvyeahxoefkeexmdowryxqfodfllistmmkmxearbtyyxzletg[illegible]ozuulnn55

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生成