南明离火

——移动应用检测平台——

ANDROID 静态分析报告

Backup • v16.25

分析日期: 2025-11-21 16:59:20

应用概览

文件名称:	Backup v16.25.apk
文件大小:	16.03MB
应用名称:	Backup
软件包名:	com.spap.alarm
主活动:	com.spap.alarm.MainActivity
版本号:	16.25
最小SDK:	19
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:	40/100(中风险)
杀软检测:	7个杀毒软件报毒
MD5:	c9c09d21e70357a0d3bce86fb6d9e73a
SHA1:	22259b32cb3d01c9056e5489d012df6441c54326
SHA256:	33a0a5717b3050868d17c5cc671b9aee19894c60a4024a4c3b55ad108e4645bb

分析结果严重性分布

高危	中危	信息	安全	关注
11	30	2	2	0

四大组件导出状态统计

Activity组件：15个，其中export的有： 3个
Service组件：29个，其中export的有： 6个
Receiver组件：32个，其中export的有： 14个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

未检测到签名证书
v1 签名: False
v2 签名: False
v3 签名: False
v4 签名: False

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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。

android.permission.WRITE_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_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.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.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.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.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。
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
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。

本报告由南明离火移动安全分析平台生成

android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
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.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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.ACCESS_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.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_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.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.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.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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.hardware.camera.autofocus	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
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.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_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。

android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.VOICE_COMMUNICATION	未知	未知权限	来自 android 引用的未知权限。
android.permission.CAMCORDER	未知	未知权限	来自 android 引用的未知权限。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.ACCESS_RESTRICTED_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
com.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。

本报告由南明离火移动安全分析平台生成

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全分析

高危: **1** | 警告: **0** | 信息: **0**

标题	严重程度	描述信息
缺少代码签名证书	高危	未检测到代码签名证书，存在安全风险。

Manifest 配置安全分析

高危: **10** | 警告: **25** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	Activity (com.spap.alarm.MainActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity (com.spap.alarm.MainActivity) 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 (com.spap.alarm.AliasActivity) 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 (com.spap.alarm.CheckWarnings) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
6	Activity (com.spap.alarm.activities.EnableAccesibilityAccess) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
7	Activity (com.spap.alarm.activities.AllowExternalStorage) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
8	Activity (com.spap.alarm.activities.DisableNotification) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
9	Activity (com.spap.alarm.activities.DisableNotificationOld) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
10	Activity (com.spap.alarm.other.Act_other) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

本报告由南明离火移动安全分析平台生成

11	Activity-Alias (com.spap.alarm.AliasActivity1) 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。
12	Activity (com.spap.alarm.activities.EnableNotificationAccess) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
13	Activity (com.spap.alarm.activities.PhoneAlreadyRegistered) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
14	Activity (com.spap.alarm.activities.ThankYouForRegistering) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
15	Broadcast Receiver (com.spap.alarm.MySetupBoot) 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。
16	Broadcast Receiver (com.spap.alarm.PhoneCallReceiver) 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。

17	Broadcast Receiver (com.spap.alarm.SMSReceiver) 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。
18	Broadcast Receiver (com.spap.alarm.ChangedRingerMode) 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。
19	Broadcast Receiver (com.spap.alarm.MMSReceiver) 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。
20	Broadcast Receiver (com.spap.alarm.ScreenChancedReceiver) 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 (com.spap.alarm.MyNetworkChangeReceiver) 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。

22	Broadcast Receiver (com.spap.alarm.PackageChangeReceiver) 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 (com.spap.alarm.CalendarChangedReceiver) 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 (com.spap.alarm.DeviceAdminSampleReceiver) 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。

25	Service (com.spap.alarm.services.MyNotificationListener) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_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。
26	Service (com.spap.alarm.services.MyAccessibilityService) 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。
27	Service (com.spap.alarm.receivers.MyFirebaseInstanceIDService) 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。
28	Broadcast Receiver (com.spap.alarm.receivers.MyPluginControlReceiver) 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。

本报告由南明离火移动安全分析平台生成

29	Service (com.spap.alarm.services.MyWorkerServerCom) 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。
30	Service (com.spap.alarm.services.MyFirebaseMessagingService) 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。
31	Broadcast Receiver (com.spap.alarm.receivers.MySystemCalls) 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。
32	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。

本报告由南明离火移动安全分析平台生成

33	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。
34	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。
35	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: **0** | 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

本报告由南明离火移动安全分析平台生成

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
3	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

4	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
5	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

应用行为分析

编号	行为	标签	文件
00208	捕获设备屏幕的内容	信息收集 屏幕	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
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
00045	查询当前运行的应用程序名称	信息收集 反射	升级会员：解锁高级权限
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
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

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
00056	修改语音音量	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
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
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限

00091	从广播中检索数据	信息收集	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
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
00044	查询该包的activity上次被使用的时间	信息收集 反射	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00102	将手机扬声器设置为打开	命令	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
00130	获取当前WIFI信息	WiFi 信息收集	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00002	打开相机并拍照	相机	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
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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	19/30	android.permission.READ_PHONE_STATE android.permission.RECEIVE_SMS android.permission.READ_SMS android.permission.ACCESS_COARSE_LOCATION android.permission.READ_CALENDAR android.permission.RECORD_AUDIO android.permission.PROCESS_OUTGOING_CALLS android.permission.WRITE_CALL_LOG android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.ACCESS_FINE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.CAMERA android.permission.RECEIVE_MMS android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.PACKAGE_USAGE_STATS
其它常用权限	14/46	android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.BLUETOOTH android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH_ADMIN android.permission.FLASHLIGHT android.permission.BROADCAST_STICKY android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE

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.sappmonitoring.com	安全	否	No Geolocation information available.
appr.tc	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
studio131-8250f.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://apprtc	org/appspot/apprtc/RoomParametersFetcher.java
• https://appr.tc	org/appspot/apprtc/util/AsyncHttpURLConnection.java
• https://www.google.com	de/tavendo/autobahn/WebSocketWriter.java
• www.*!!*@@!6*!!*@@!5!!*@@9*!!*@@!5	com/spap/alarm/fsgrgrh.java

• www.!!*@@9*!!*@@!5*!!*@@!5-#@@@.c*!!*@@!8m/	com/spap/alarm/greger.java
• www.*!!*@@!6*!!*@@!5!!*@@9*!!*@@!5	com/spap/alarm/activities/dsgdfh.java
• www.*!!*@@!6*!!*@@!5!!*@@9*!!*@@!5	com/spap/alarm/activities/gdfhhh.java
• www.s*!!*@@!5y-d!!*@@9t!!*@@9c*!!*@@!4nt*!!*@@!4*!!*@@!7.c*!!*@@!8m/*!!*@@!6*!!*@@!4nd_d!!*@@9t!!*@@9.*!!*@@!5h*!!*@@!5	com/spap/alarm/teee/gergerg.java
• https://appr.tc • www.!!*@@9*!!*@@!5*!!*@@!5-#@@@.c*!!*@@!8m/ • https://firebase.google.com/support/privacy/init-options • www.*!!*@@!6*!!*@@!5!!*@@9*!!*@@!5 • https://www.sappmonitoring.com/invite/download.apk • https://www.google.com • https://%s/%s/%s • https://studio131-8250f.firebaseio.com • www.s*!!*@@!5y-d!!*@@9t!!*@@9c*!!*@@!4nt*!!*@@!4*!!*@@!7.c*!!*@@!8m/*!!*@@!6*!!*@@!4nd_d!!*@@9t!!*@@9.*!!*@@!5h*!!*@@!5	白研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://studio131-8250f.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/172739220163/namespaces/firebase:fetch?key=AIzaSyC_dtESjgMaokaWHc5c3oxoGH70etKsCyM ） 已禁用。响应内容如下所示：
		
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
WebRTC	WebRTC	借助 WebRTC，您可以在基于开放标准的应用程序中添加实时通信功能。它支持在同级之间发送视频，语音和通用数据，从而使开发人员能够构建功能强大的语音和视频通信解决方案。该技术可在所有现代浏览器以及所有主要平台的本机客户端上使用。 WebRTC 背后的技术被实现为一个开放的 Web 标准，并在所有主要浏览器中均以常规 JavaScript API 的形式提供。
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。
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。

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
"firebase_database_url" : "https://studio131-8250f.firebaseio.com"
"google_api_key" : "AIzaSyC_dtESjgMaokaWHc5c3oxoGH70etKsCyM"
"google_app_id" : "1:172739220163:android:ae174a2dce4e9348"
"google_crash_reporting_api_key" : "AIzaSyC_dtESjgMaokaWHc5c3oxoGH70etKsCyM"
"password" : "Password"
"pref_aecdump_key" : "aecdump_preference"
"pref_audiocodec_key" : "audiocodec_preference"
"pref_audiosettings_key" : "audio_settings_key"
"pref_camera2_key" : "camera2_preference"
"pref_capturequalityslider_key" : "capturequalityslider_preference"
"pref_data_id_key" : "data_id_preference"
"pref_data_protocol_key" : "Subprotocol"
"pref_datasettings_key" : "data_settings_key"
"pref_disable_built_in_aec_key" : "disable_built_in_aec_preference"
"pref_disable_built_in_agc_key" : "disable_built_in_agc_preference"

"pref_disable_built_in_ns_key" : "disable_built_in_ns_preference"
"pref_disable_webrtc_agc_and_hpf_key" : "disable_webrtc_agc_and_hpf_preference"
"pref_displayhud_key" : "displayhud_preference"
"pref_enable_datachannel_key" : "enable_datachannel_preference"
"pref_enable_rtceventlog_key" : "enable_rtceventlog_key"
"pref_enable_save_input_audio_to_file_key" : "enable_key"
"pref_flexfec_key" : "flexfec_preference"
"pref_fps_key" : "fps_preference"
"pref_hwcodec_key" : "hwcodec_preference"
"pref_max_retransmit_time_ms_key" : "max_retransmit_time_ms_preference"
"pref_max_retransmits_key" : "max_retransmits_preference"
"pref_maxvideobitrate_key" : "maxvideobitrate_preference"
"pref_maxvideobitratevalue_key" : "maxvideobitratevalue_preference"
"pref_miscsettings_key" : "misc_settings_key"
"pref_negotiated_key" : "negotiated_preference"
"pref_noaudioprocessing_key" : "audioprocessing_preference"
"pref_opensles_key" : "opensles_preference"
"pref_ordered_key" : "ordered_preference"
"pref_resolution_key" : "resolution_preference"
"pref_room_key" : "room_preference"

"pref_room_list_key" : "room_list_preference"
"pref_room_server_url_key" : "room_server_url_preference"
"pref_screencapture_key" : "screencapture_preference"
"pref_speakerphone_key" : "speakerphone_preference"
"pref_startaudiobitrate_key" : "startaudiobitrate_preference"
"pref_startaudiobitratevalue_key" : "startaudiobitratevalue_preference"
"pref_tracing_key" : "tracing_preference"
"pref_use_legacy_audio_device_key" : "use_legacy_audio_device_key"
"pref_videocall_key" : "videocall_preference"
"pref_videocodec_key" : "videocodec_preference"
"pref_videosettings_key" : "video_settings_key"
"password" : "Contrasenya"
"password" : "Adgangskode"
"password" : "Passwort"
"password" : "Wagwoord"
"password" : "Salasana"
"password" : "Heslo"
"password" : "Wachtwoord"
"password" : "Geslo"
"password" : "Pasword"

"password" : "Passord"
"password" : "Parola"
"password" : "Heslo"
"password" : "Parool"
"password" : "Password"
"password" : "Palavra-passe"
"password" : "Parole"
"password" : "Nenosiri"
"password" : "Parol"
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b

免责声明及风险提示: