南明离火
移动应用检测平台

ANDROID 静态分析报告

ADMIN SERVER • v1.0

分析日期: 2025-07-06 09:51:40

应用概览

文件名称:	03b3a62fdeff156a7d4c6fa2dc71fd61d8fce79b1bfc3b2c6b0c7e6075c53708 v1.0.apk
文件大小:	8.41MB
应用名称:	ADMIN SERVER
软件包名:	com.pubgm
主活动:	com.pubgm.activity.LoginActivity
版本号:	1.0
最小SDK:	28
目标SDK:	35
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:	3 个杀毒软件报毒
MD5:	d2d7462eab9ef7e28cb2aea576c8d38c
SHA1:	18ceef99b391e17872178fb187a9ca2fb098a8c7
SHA256:	03b3a62fdeff156a7d4c6fa2dc71fd61d8fce79b1bfc3b2c6b0c7e6075c53708

分析结果严重性分布

高危	中危	信息	安全	关注
0	82	1	1	0

四大组件导出状态统计

Activity组件：56个，其中export的有： 3个
Service组件：26个，其中export的有： 0个
Receiver组件：2个，其中export的有： 2个
Provider组件：27个，其中export的有： 24个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: False
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.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.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.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.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.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.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。
android.permission.HIDE_OVERLAY_WINDOWS	普通	隐藏应用叠加窗口	允许应用防止在其上绘制非系统覆盖窗口。
android.permission.QUERY_ADVANCED_PROTECTION_MODE	未知	未知权限	来自 android 引用的未知权限。
android.permission.DUMP	签名(系统)	获得系统内部状态	允许应用程序检索系统的内部状态。恶意应用程序可借此检索它们本不需要的各种保密信息和安全信息。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。

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.facebook.services.identity.FEO2	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.talk.permission.READ_ONLY	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.talk.permission.WRITE_ONLY	未知	未知权限	来自 android 引用的未知权限。
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.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动
com.google.android.gms.permission.AD_ID_NOTIFICATION	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.FOREGROUND_SERVICE_CAMERA	签名	允许使用相机的前台服务	它允许应用程序在前台服务中访问摄像头，例如支持多任务的视频聊天应用。这个权限只能由系统授予，不能由用户授予
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	普通	通过连接的设备使用启用前台服务	允许常规应用程序使用类型为“connectedDevice”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_HEALTH	普通	启用具有健康相关功能的前台服务	允许常规应用程序使用类型为“health”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
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.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.FOREGROUND_SERVICE_MICROPHONE	普通	允许使用麦克风的前台服务	允许常规应用程序使用类型为“麦克风”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_PHONE_CALL	普通	在通话期间启用前台服务	允许常规应用程序使用类型为“phoneCall”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	普通	允许前台服务进行远程消息传递	允许常规应用程序使用类型为“remoteMessaging”的 Service.startForeground。

本报告由南明离火移动安全分析平台生成

android.permission.FOREGROUND_SERVICE_SPECIAL_USE	普通	启用特殊用途的前台服务	允许常规应用程序使用类型为“specialUse”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	普通	允许系统豁免类型的前台服务	允许常规应用程序使用类型为“systemExempted”的 Service.startForeground。仅允许应用程序在 ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED 中列出的用例中使用此类型。
com.open.gallery.smart.Read	未知	未知权限	来自 android 引用的未知权限。
android.permission.HIGH_SAMPLING_RATE_SENSORS	普通	传感器的数据刷新率限制	允许应用以大于 200 Hz 的采样率访问传感器数据，此数据包括由设备的加速度，陀螺仪和磁力传感器记录的值。
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.ACCEPT_HANDOVER	危险	使呼叫应用程序能够继续在另一个应用程序中启动的呼叫	允许呼叫应用程序继续在另一个应用程序中发起的呼叫。例如，一个视频通话应用程序希望在用户的移动网络上继续语音通话。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
android.permission.BODY_SENSORS_BACKGROUND	危险	授予对身体传感器的后台访问权限，例如心率	允许应用程序访问来自传感器的数据，用户使用这些传感器来测量体内发生的事情，例如心率。如果您正在请求此权限，则还必须请求。
android.permission.UWB_RANGING	危险	使用超宽带对设备进行测距所需	需要能够使用超宽带覆盖设备。
android.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
android.permission.DETECT_SCREEN_CAPTURE	普通	允许尝试对应用程序窗口进行屏幕捕获时发出通知。	允许应用程序在尝试对其窗口进行屏幕捕获时收到通知。
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。
ohos.permission.GET_BUNDLE_INFO	未知	未知权限	来自 android 引用的未知权限。
android.permission.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
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_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.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.ACCESS_MEDIA_LOCATION	危险	获取照片的地址信息	更换头像，聊天图片等图片的地址信息被读取。
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.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.RUN_USER_INITIATED_JOBS	普通	允许使用用户启动的作业 API	允许应用程序使用用户启动的作业 API。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.WRITE_SOCIAL_STREAM	危险	写入用户社会流	允许应用程序读写用户社会流。
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_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.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.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.WRITE_PROFILE	危险	写入用户资料	允许应用程序 读写用户个人信息。
android.permission.READ_USER_DICTIONARY	危险	读取用户定义的词典	允许应用程序读取用户在用户词典中存储的任意私有字词、名称和短语。
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.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.SUBSCRIBED_FEEDS_READ	普通	读取订阅信息	允许应用程序读取订阅信息。
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_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。
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.SUBSCRIBED_FEEDS_WRITE	危险	读取订阅信息	允许应用程序读取订阅信息。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
android.permission.READ_SOCIAL_STREAM	危险	读取用户的社交信息流	允许应用程序读取用户的社交信息流。
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.BODY_SENSORS	危险	授予对身体传感器的访问权限，例如心率	允许应用程序访问来自传感器的数据，用户使用这些传感器来测量身体内部发生的事情，例如心率。
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.WRITE_USER_DICTIONARY	普通	写入用户定义的词典	允许应用程序向用户词典中写入新词。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
android.permission.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
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.TRANSMIT_IR	普通	允许使用设备的红外发射器	允许使用设备的红外发射器（如果可用）。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
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.READ_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
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.RECEIVE_WAP_PUSH	危险	接收WAP	允许应用程序接收和处理 WAP 信息。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_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
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.SET_WALLPAPER_HINTS	普通	设置壁纸大小	允许应用程序设置壁纸大小。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
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.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.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
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.READ_CONTACTS	危险	读取联系人信息	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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.READ_SYNC_STATS	普通	读取同步统计信息	允许应用程序读取同步统计信息；例如已发生的同步历史记录。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.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.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.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_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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.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.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.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.NEARBY_WIFI_DEVICES	危险	需要通过 Wi-Fi 进行广告和连接到附近的设备	需要能够通过 Wi-Fi 进行广告宣传和连接到附近的设备。
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.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_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.USE_SIP	危险	收听/发出网络电话	允许应用程序使用SIP服务拨打接听互联网通话。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	在后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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。
com.pubgm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
top.bienvenido.mundo.FBLoginAbility	Schemes: fbconnect://,

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: **79** | 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。
3	Activity (com.pubgm.activity.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 (top.bienvenido.mundo.manifest.MundoIntermediary) 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 (top.bienvenido.mundo.FBLoginAbility) 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 (top.bienvenido.mundo.manifest.MundoReceiver) 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。
7	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB1)	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）。

8	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB2)	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）。
9	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB3)	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）。
10	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB4)	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 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB5)	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）。
12	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB6)	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）。
13	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB7)	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）。
14	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB8)	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）。
15	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB9)	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）。
16	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB10)	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）。
17	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB11)	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）。

18	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB12)	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）。
19	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB13)	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）。
20	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB14)	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）。
21	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB15)	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）。
22	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB16)	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）。
23	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB17)	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）。
24	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB18)	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）。
25	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB19)	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）。
26	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB20)	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）。
27	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB21)	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）。

28	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB22)	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 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB23)	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）。
30	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB24)	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）。
31	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB1H)	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）。
32	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB2H)	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）。
33	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB3H)	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）。
34	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB4H)	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）。
35	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB5H)	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）。
36	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB6H)	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）。
37	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB7H)	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）。

38	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB8H)	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）。
39	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB9H)	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）。
40	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB10H)	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）。
41	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB11H)	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）。
42	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB12H)	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）。
43	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB13H)	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）。
44	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB14H)	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）。
45	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB15H)	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）。
46	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB16H)	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）。
47	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB17H)	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）。

48	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB18H)	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）。
49	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB19H)	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）。
50	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB20H)	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）。
51	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB21H)	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）。
52	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB22H)	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）。
53	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB23H)	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）。
54	Activity 设置了 TaskAffinity 属性 (top.bienvenido.mundo.manifest.MundoActivity$Companion$STUB24H)	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）。
55	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB1) 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。
56	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB2) 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。
57	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB3) 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。

本报告由南明离火移动安全分析平台生成

58	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB4) 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。
59	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB5) 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。
60	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB6) 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。
61	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB7) 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。
62	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB8) 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。
63	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB9) 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。
64	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB10) 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。
65	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB11) 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。
66	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB12) 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。
67	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB13) 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。

68	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB14) 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。
69	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB15) 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。
70	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB16) 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。
71	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB17) 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。
72	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB18) 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。
73	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB19) 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。
74	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB20) 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。
75	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB21) 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。
76	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB22) 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。
77	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB23) 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。

78	Content Provider (top.bienvenido.mundo.manifest.MundoProvider$Companion$STUB24) 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。
79	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。

代码安全漏洞检测

高危: **0** | 警告: **2** | 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

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/libclient.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，以便它会对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: ['__vsprintf_chk', '__vsnprintf_chk']	True info 符号被剥离

2	arm64-v8a/libmxlct43f6hkf.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: ['__memcpy_chk', '__vsprintf_chk', '__memset_chk', '__read_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
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
00104	检查给定路径是否是目录	文件	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
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
00079	隐藏当前应用程序的图标	规避	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
00091	从广播中检索数据	信息收集	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
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
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
00024	Base64解码后写入文件	反射 文件	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
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
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
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
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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	27/30	android.permission.PACKAGE_USAGE_STATS android.permission.ACCEPT_HANDOVER android.permission.RECEIVE_SMS android.permission.CALL_PHONE android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_CALL_LOG android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.ACCESS_FINE_LOCATION android.permission.WRITE_CALENDAR android.permission.SYSTEM_ALERT_WINDOW android.permission.RECORD_AUDIO android.permission.GET_ACCOUNTS android.permission.RECEIVE_MMS android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.WAKE_LOCK android.permission.WRITE_CONTACTS android.permission.WRITE_CALL_LOG android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CALENDAR android.permission.SET_WALLPAPER android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.SEND_SMS android.permission.READ_SMS
其它常用权限	23/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.RECORD_AUDIO com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACTIVITY_RECOGNITION android.permission.ACCESS_BACKGROUND_LOCATION android.permission.FLASHLIGHT android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.BROADCAST_STICKY android.permission.AUTHENTICATE_ACCOUNTS android.permission.CHANGE_WIFI_STATE android.permission.READ_MEDIA_VIDEO android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
raw.githubusercontent.com	安全	否	**IP地址:** 185.199.111.133 **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
www.62v.net	安全	否	**IP地址:** 104.21.22.153 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
vipsververrpanel.xyz	安全	否	**IP地址:** 104.21.64.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://www.62v.net/jnative/binder	l2/f.java
• https://www.62v.net/jnative/binder	k4/o3.java
• https://raw.githubusercontent.com/hkgjdh/hk-cheats-load/v2/main/download.php	f2/m.java
• ftp://%s:%s@%s • https://vipsververrpanel.xyz/api/login • 1.2.0.4	lib/arm64-v8a/libclient.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

邮箱地址敏感信息提取

EMAIL	源码文件
help@62v.net	k4/r.java

敏感凭证泄露检测

可能的密钥
b80f5549d3fb49cbb5ced644e77f218fdb73df2526105f90deb5295bc9da52c4e0d82a382c4cbcc393c400008638ea7786be7d9dd0e4383cec1329bf07188c005b9514b07755c8993b66363890079bd567835806c3441d66322e947d1d77b60b
86042823c6197eb33d7d6a65a627469dbc3e90f2e24632ce62e945fd50b021f349739fa7459ed5d10d2846c028afe34d
9250221494edbb8ddfe1dbf7cfaadd434a4998ebe11d84b8fcf5af24b0b335eb4f9c545fa077c370ded703ff9b6d60681a71ac9e4c8be08955f57aaa83f011e
37e41a97f6a8ef509c6669dafc9c29a7
b80f5549d3fb49cbb5ced644e77f218fdb73df2526105f90deb5295bc9da52c4e0d82a382c4cbcc393c400008638ea7786be7d9dd0e4383cec1329bf07188c009d4ed1f8ad2b0d8541431e54471f051367835806c3441d66322e947d1d77b60b
b80f5549d3fb49cbb5ced644e77f218f6d0b5f1c2ea9534923e4d3dff02aad443131aea202790a307b4cc4f26563a722
f221ad5694a99ff2cfd2518512661c60
2379a0fb1cc59a8a0d85cce27facd00f91f722b2ddbdc99a168879abe1c5741fe909c6edbd8e6ad846ed7307178ae4cdb6b169dfb32ea70f830cbc4fe86abe3a
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b30090603550406130255533113301106035504081 30a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bf724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1e0bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
b53ff26c044972b8f1567032ae6f80694107dfbb66ec2cd118275facb4b7ed3452c67a428279f5e22c444f896581e06bef45977394fbe18ecde2a4ea255c6ae8
5cc986ddbe0bc13f88e24c504b96d1110c503676f005773c2651c932582ec87d757531a0a2b970616faf54e0c9d95991
3c380e0df24a9aec04f367bcbab97a01

0276a1615185e03ac1af12b79a0d34ed572f5ae2f997205e08683daf2dc45b54570d4b0a8c17ebd26fd2ea20b9819401
b80f5549d3fb49cbb5ced644e77f218fdb73df2526105f90deb5295bc9da52c4e0d82a382c4cbcc393c400008638ea7786be7d9dd0e4383cec1329bf07188c0080fc583c9b9606d90003e7f97ef971e767835806c3441d66322e947d1d77b60b

免责声明及风险提示: