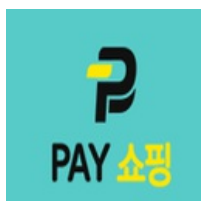




ANDROID 静态分析报告



• PAY

• v2.0.5

分析日期: 2025-04-08 13:06:43

i应用概览

文件名称:	PAY v2.0.5.apk
文件大小:	22.1MB
应用名称:	PAY
软件包名:	com.buntya.april18
主活动:	com.buntya.april18.activity.MainActivity
版本号:	2.0.5
最小SDK:	21
目标SDK:	22
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
杀软检测:	28 个杀毒软件报毒
MD5:	b5b1a0b8e0b0e3b6fcf857736c773d68
SHA1:	97e2e30459d0a96e2ec6422d9f3e1532f301c78
SHA256:	e66534171d9845e8de8612529f66d2e787ed84bb01a52d0adbd0779cb258c33

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
2	17	1	2	2

📦 四大组件导出状态统计

Activity组件: 4个, 其中export的有: 1个
Service组件: 14个, 其中export的有: 6个
Receiver组件: 14个, 其中export的有: 6个
Provider组件: 3个, 其中export的有: 0个

🌿 应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=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: 2008-04-15 22:40:50+00:00
有效期至: 2035-09-01 22:40:50+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: 0xb3998086d056cffa
哈希算法: md5
证书MD5: 8ddb342f2da5408402d7568af21e29f9
证书SHA1: 27196e386b875e76adf700e7ea84e4c6eee33dfa
证书SHA256: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
证书SHA512:
5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6ef602d45d1a2ebae9f002a6598e72fd2d83

公钥算法: rsa
密钥长度: 2048
指纹: 65ba0830722d5767f8779e37d0d9c67562f03ec63a2889af655ee9c59effb434
找到 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.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摄的图像。
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.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.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.BOOT_COMPLETED	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.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.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.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.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.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.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.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.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。
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.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
android.permission.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.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_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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.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.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.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.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.RECEIVE_LAUNCH_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
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.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
com.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.buntia.april18.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.buntia.april18.activity.CallActivity	Schemes: tel://,

网络通信安全风险

序号	范围	严重级别	描述
----	----	------	----

证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

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

Manifest 配置安全分析

高危: 1 | 警告: 16 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
----	----	------	------

1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Service (com.buntya.april18.service.GTService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
5	Broadcast Receiver (com.buntya.april18.receiver.CallReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
6	Broadcast Receiver (com.buntya.april18.receiver.RebootReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
7	Broadcast Receiver (com.buntya.april18.receiver.MegReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
8	Service (com.buntya.april18.service.AutoTaskService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
9	Service (com.buntya.april18.service.CallService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_INCALL_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
10	Activity (com.buntya.april18.activity.CallActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

11	Service (com.google.firebase.messaging.FirebaseMessagingService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
14	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
15	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.RECEIVE [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
16	Service (com.google.firebase.iid.FirebaseInstanceIdService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
17	高优先级的Intent (2147483647) - {2} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖其他请求。

代码安全漏洞检测

高危: 1 | 警告: 0 | 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	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

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	armeabi-v7a/libdn_ssl.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No ne 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	armeabi-v7a/libfirebase.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No ne 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	armeabi-v7a/liblive.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。	No ne inf o 二进制文件没有设置运行时搜索路径或RPATH	N o n e i n f o 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。	Tr u e i n f o 符号被剥离
4	armeabi-v7a/libZegoExpressEngine.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。	No n e i n f o 二进制文件没有设置运行时搜索路径或RPATH	N o n e i n f o 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。	Tr u e i n f o 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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

00104	检查给定路径是否是目录	文件	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.CAMERA android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.PROCESS_OUTGOING_CALLS android.permission.VIBRATE android.permission.READ_CONTACTS android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_SMS android.permission.CALL_PHONE android.permission.RECEIVE_SMS android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_CONTACTS android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	14/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.BROADCAST_STICKY android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 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
lame.sf.n	安全	否	IP地址: 104.18.21.237 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

docs.zegocloud.com	安全	是	IP地址: 47.242.198.129 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图
doc-zh.zego.im	安全	是	IP地址: 47.103.157.124 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468944 查看: 高德地图
www.videolan.org	安全	否	IP地址: 13.36.253.2 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
http://www.videolan.org/x264.html	lib/armeabi-v7a/liblive.so
1.3.101.112 127.0.0.1 - file://localhost - https://docs.zegocloud.com/article/7612 1.4.0.46 - https://doc-zh.zego.im/article/13610#1 1.3.101.110 1.2.0.4 - http://lame.sf.net - ftp://%s:%s@%s - https://doc-zh.zego.im/article/9670 - https://doc-zh.zego.im/article/1153	lib/armeabi-v7a/libZegoExpressEngine.so

🔌 Firebase 配置安全检测

标题	严重程度	描述信息
Firebase远程配置已禁用	安全	Firebase远程配置URL (https://firebaseremoteconfig.googleapis.com/v1/projects/413012109604/namespaces/firebase:fetch?key=AlzaSyDLXr-N-u0VuKmhxGyxXCOxIa6wOdKEL4E) 已禁用。响应内容如下所示: <pre>{ "state": "NO_TEMPLATE" }</pre>

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
Realm	Realm	Realm 平台是一个用于跨平台应用程序的次世代数据层。Realm 是响应式的、并发的和轻量级的，它允许您使用实时的原生对象。使用 Realm 可使您的应用程序在信号较弱、脱机或中断的情况下无缝运行。
即构极速视频 SDK	即构	极速视频（Express Video）是一款实时的音视频互动服务产品，能够为开发者提供便捷接入、高可靠、多平台互通的音视频服务。通过低至 200 ms 的端到端平均时延，业内领先的保障弱网质量的 QoS 策略，并结合强大的 3A 处理能力，完美支持一对多、多对多的实时音视频通话、直播、会议等场景。

敏感凭证泄露检测

可能的密钥
凭证信息=> "key": "dbcdcfghijkltiyr"
"google_app_id": "1:413012109604:android:1c6bc275033cfd96cbabb1"
"google_api_key": "AlzaSyDLXr-N-u0VuKmhxGyxXCOxla6wOdKEL4E"
"google_crash_reporting_api_key": "AlzaSyDLXr-N-u0VuKmhxGyxXCOxla6wOdKEL4E"

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成