



ANDROID 静态分析报告



惠州公积金 · v1.1

分析日期: 2024-06-06 22:22:27

i应用概览

文件名称:	hgzjrrj.apk
文件大小:	21.64MB
应用名称:	惠州公积金
软件包名:	com.huizhou.gjj.huizhougjj
主活动:	com.huizhou.gjj.huizhougjj.WelcomeActivity
版本号:	1.1
最小SDK:	19
目标SDK:	27
加固信息:	360加固 加固
应用程序安全分数:	34/100 (高风险)
跟踪器检测:	4/432
杀软检测:	10 个杀毒软件报毒
MD5:	48e3601d07c73758582864317959d084
SHA1:	9a048470c15f60ba95d8aa8441e182a6fcc9e089
SHA256:	d5733a143a6a32e8d0093903ed76028d62d19c4dc195e95eba78db3b9fd8557eb

分析结果严重性分布

高危	中危	信息	安全	关注
11	18	1	1	2

四大组件导出状态统计

Activity组件: 63个, 其中export的有: 1个
Service组件: 4个, 其中export的有: 2个
Receiver组件: 4个, 其中export的有: 1个
Provider组件: 3个, 其中export的有: 1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: CN=huizhougj
签名算法: rsassa_pkcs1v15
有效期自: 2019-11-19 01:32:47+00:00
有效期至: 2044-11-12 01:32:47+00:00
发行人: CN=huizhougj
序列号: 0x280ef473
哈希算法: sha256
证书MD5: 60004988d5daf1459f8b243b33730c5
证书SHA1: 0c5aab2d53b710eaa3ce34899ae0833ca9aafb43
证书SHA256: 0f3208c5495f98eb7282520585c236c4eb284e1c0b304b4d42535e738d96c450
证书SHA512:
f1d75a28f27c23b9e07f417191e0a5f6ec53734cbc2911ab6da40a3eb89c0b1e5ee3b3d3cb815802129c7b6a50164d6b1128dd91f02daab38a88af5a698c3a9c

公钥算法: rsa
密钥长度: 2048
指纹: ccb1a54a00d4862c90bd374d38fd945d8320157794332928f7d08655dfd908ea
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
com.huizhou.gjj.huizhougj.permission.JPUSH_MESS AGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.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.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_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.ACCESS_DOWNLOAD_MANAGER	签名(系统)	访问下载管理器	这个权限是允许应用访问下载管理器，以便管理大型下载操作。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	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.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.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.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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除密码之类的操作。
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.ACTION_MEDIA_SCANNER_SCAN_FILE	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_GPS	签名(系统)	使用GPS权限	这个权限已经被废弃，不再被系统支持。这个权限曾经用于访问GPS位置，但是现在已经被android.permission.ACCESS_FINE_LOCATION替代。
android.permission.BAIDU_LOCATION_SERVICE	未知	未知权限	来自 android 引用的未知权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.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错略的经纬度信息，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.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.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。
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.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.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。

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: 1 | 信息: 1

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

Manifest 配置安全分析

高危: 7 | 警告: 8 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	Activity (com.huizhou.gjj.huizhougjj.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance", 因为这会使其成为根 Activity, 并可能导致其他应用程序读取调用 Intent 的内容。因此, 当 Intent 包含敏感信息时, 需要使用 "standard" 启动模式属性。
4	Activity (com.huizhou.gjj.huizhougjj.MainActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后, 其他应用程序可以将恶意活动放置在活动栈顶部, 从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.huizhou.gjj.huizhougjj.function.hz.activity.LoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance", 因为这会使其成为根 Activity, 并可能导致其他应用程序读取调用 Intent 的内容。因此, 当 Intent 包含敏感信息时, 需要使用 "standard" 启动模式属性。
6	Activity (com.huizhou.gjj.huizhougjj.function.hz.activity.LoginActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后, 其他应用程序可以将恶意活动放置在活动栈顶部, 从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 28 或更高版本以在平台级别修复此问题。
7	Activity (com.huizhou.gjj.huizhougjj.function.hz.activity.qywActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance", 因为这会使其成为根 Activity, 并可能导致其他应用程序读取调用 Intent 的内容。因此, 当 Intent 包含敏感信息时, 需要使用 "standard" 启动模式属性。
8	Activity (com.huizhou.gjj.huizhougjj.function.hz.activity.TownActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后, 其他应用程序可以将恶意活动放置在活动栈顶部, 从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 28 或更高版本以在平台级别修复此问题。

9	Service (cn.jpush.android.service.DaemonService) 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。
10	Content Provider (cn.jpush.android.service.DownloadProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
11	Activity设置了TaskAffinity属性 (cn.jpush.android.service.JNotifyActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
12	Activity (cn.jpush.android.service.JNotifyActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的启动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (cn.jpush.android.service.JNotifyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
14	Service (com.huizhou.gjj.huizhougjj.push.PushService) 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。
15	Broadcast Receiver (com.huizhou.gjj.huizhougjj.push.MyPushMessageReceiver) 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。
16	高优先级的Intent (1000) [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了其他请求。

代码安全漏洞检测

高危: 4 | 警告: 8 | 信息: 1 | 安全: 1 | 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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 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
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	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
7	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: 默认权限不严格 OWASP Top 10: M2: Improper Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	可能存在跨域漏洞。在WebView中启用从URL访问文件可能会泄露文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
9	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
10	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

11	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
12	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
13	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
14	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

🚩 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)	SYMBOL STRIPPED (裁剪符号表)
----	-----	------------	-----	-------------------	-------	------------------	--------------------	-------------------	-------------------------

1	armeabi/libdeviceid_1.0.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。		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。	N o n e info 二进制文件没有设置运行时的搜索路径或 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	Fa ls e w a r n i n g 符 号 可 用
2	armeabi/libmodft2.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。		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。	N o n e info 二进制文件没有设置运行时的搜索路径或 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	Fa ls e w a r n i n g 符 号 可 用

3	armeabi/libtoyger.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。		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。	N o n e i n f o 二进制文件没有设置运行搜索路径或 RUNPATH	/Users/wangweiwei/Library/Android/sdk/ndk-bundle/toolchains/llvm/prebuilt/darwin-x86_64/lib64/clang/5.0.300080/lib/linux/arm high 二进制文件设置了 RUNPATH。在某些情况下，攻击者可以滥用这个特性或者修改环境变量来运行任意的库，从而实现代码执行和权限提升。库应该设置 RUNPATH 的唯一时间是当它链接到同一个包中的私有库时。移除编译选项 --enable-new-dtags, rpath 来移除 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	Fa l s e w a r n i n g 符号可用
4	armeabi/libwebpbackport.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。		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。	N o n e i n f o 二进制文件没有设置运行搜索路径或 RUNPATH	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	Fa l s e w a r n i n g 符号可用

5	armeabi/libX86Bridge.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。	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。	N o n e i n f o 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	Fa l s e w a r n i n g 符号可用
---	-------------------------	---	--	--	--	---	--	--

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	12/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.WRITE_SETTINGS android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	11/46	android.permission.BLUETOOTH android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.CHANGE_NETWORK_STATE android.permission.BROADCAST_STICKY

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.intel.com	安全	否	IP地址: 23.49.157.210 国家: 大韩民国 地区: 首尔teukbyeolsi 城市: 首尔 纬度: 37.566311 经度: 126.977203 查看: Google 地图
wsbs.hzgjj.cn	安全	是	IP地址: 113.106.167.244 国家: 中国 地区: 广东 城市: 惠州 纬度: 39.500766 经度: 116.693001 查看: 高德地图
img.souche.com	安全	是	IP地址: 150.138.98.238 国家: 中国 地区: 山东 城市: 青岛 纬度: 36.093613 经度: 120.371941 查看: 高德地图

🌐 URL 链接安全分析

URL信息	源码文件
http://cn-hangzhou-mas-log.cloud.alipay.com	自研引擎-M
http://10.11.20.87:8080/ydnmc	com/huizhou/gjj/huizhougjj/common/CommonVariable.java
https://www.baidu.com/	com/huizhou/gjj/huizhougjj/network/Host.java
https://mapsv1.bdimg.com/scale/?qt=pdata&sid=	com/baidu/panosdk/plugin/indoor/view/IndoorAlbumView.java
- http://img.souche.com/ - http://souche.oss-cn-hangzhou.aliyuncs.com/	com/guoxiaoxing/phoenix/picker/model/PhoenixConstant.java
- http://10.11.20.87:8080/ydnmc - http://wsbs.hzgjj.cn/miapp/	com/huizhou/gjj/huizhougjj/BuildConfig.java
127.0.0.1	com/huizhou/gjj/huizhougjj/App.java
http://www.intel.com/software/products/support/	lib/armeabi/libtoyger.so

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
-------	-----	------

金融级实名认证 SDK	Alibaba	金融级实名认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
Pdfium	Google	Pdfium Android binding.
WebP	Alexey Pelykh	WebP format support for Android < 4.0.
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。JPush 全面支持 Android, iOS, Winphone 三大手机平台。
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。

 第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

 敏感凭证泄露检测

可能的密钥
凭证信息=> "appkey" : "C321516081130_ANDROID"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "t8TKngF0jKJkGy78X4P5RY8jraieuxv"
极光推送的=> "JPush_CHANNEL" : "developer-default"
mPjwVstkBCapUvny19fhgA==
IlcF4O7D2-+PwpWLXZdK1vugLz6xIU4zK0J8aSc/OfM9W8CCbh5kYEGTGF6B2+aqITbx+L76fN5fdf8CGwILmJ7s6Qm6ZXZwgvyj+Z0ttmXTd1FUynSWJIGH Gxell
559bdba1be9f105984694e11114da957
TAISxiWwpsqUdaqrR1JLHjztw==
5dee058e8fc19571190001a8
5e1744fc6856bafae4994def9ad6c46

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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成