南明离火
移动应用检测平台

# ANDROID 静态分析报告

**Maybank2 • v2.0.0**

**分析日期: 2025-04-30 21:27:01**

# 应用概览

| | |
|---|---|
| 文件名称: | Maybank2 v2.0.0.apk |
| 文件大小: | 1.5MB |
| 应用名称: | Maybank2 |
| 软件包名: | m.m.ml |
| 主活动: | m.m.ml.MainActivity |
| 版本号: | 2.0.0 |
| 最小SDK: | 24 |
| 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: | 61/100 (低风险) |
| 杀软检测: | 22 个杀毒软件报毒 |
| MD5: | e93bb4fbec2fdb20d57e3aba7c520d7a |
| SHA1: | 9aec39bec1e356a56d24da3d3118716f500c5b9f |
| SHA256: | 5008d74bf8d03bea5a79487fcfc4127840cf621eb2da90cac362c910bcd130fb |

# 分析结果严重性

| 高危 | 中危 | 低危 | 安全 | 关注 |
|---|---|---|---|---|
| 0 | 5 | 0 | 1 | 0 |

# 四大组件信息

| |
|---|
| Activity组件：1个，其中export的有：0个 |
| Service组件：1个，其中export的有：1个 |
| Receiver组件：2个，其中export的有：2个 |
| Provider组件：0个，其中export的有：0个 |

# 证书信息

二进制文件已签名
v1 签名: False
v2 签名: True

v3 签名: True
v4 签名: False
主题: C=US, ST=NY, L=New York, O=MyCompany ZqSl4UB1xI, OU=Development ZqSl4UB1xI, CN=John Doe ZqSl4UB1xI
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-20 23:25:20+00:00
有效期至: 2052-09-05 23:25:20+00:00
发行人: C=US, ST=NY, L=New York, O=MyCompany ZqSl4UB1xI, OU=Development ZqSl4UB1xI, CN=John Doe ZqSl4UB1xI
序列号: 0x50250f8a
哈希算法: sha256
证书MD5: 207c4d6615e2e5e75f5b7e157a143f34
证书SHA1: 2b92782524fbc31b60fb987e89972ccc1e5f3391
证书SHA256: b5810bcab65b5177f4bf28e48669ef24b77767063bf639a0b11431cdfcb9682e
证书SHA512:
5aa04583e29255d9c68b00b5c68c97c0fbba04a08b0e6b0cb5bda61dc4989fccde0f2b72d38d0cb6291b75e80104e8a6816a5a516ef5e15dc93180bceb90268d

公钥算法: rsa
密钥长度: 2048
指纹: 14af59fb20966a846e9194e6c57931c1da56f2350888e4faa699f2b18cf8069f
找到 1 个唯一证书

## ☰ 应用权限

| 权限名称 | 安全等级 | 权限内容 | 权限描述 |
| --- | --- | --- | --- |
| 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.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.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.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.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.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.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.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.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） |
| m.m.ml.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

| 序号 | 范围 | 严重级别 | 描述 |
|---|---|---|---|

## 证书安全分析

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 | 应用程序使用代码签名证书进行签名 |

## MANIFEST分析

高危: **0** | 警告: **5** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
|---|---|---|---|
| 1 | 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。 |
| 2 | Service (m.m.ml.SE) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.FOREGROUND_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。 |
| 3 | Broadcast Receiver (m.m.ml.RE) 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。 |
| 4 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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。 |
| 5 | 高优先级Intent （1000） - {1} 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了其他请求。 |

## 安全漏洞检测

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|---|---|---|---|---|

## 敏感权限分析

| 类型 | 匹配 | 权限 |
|---|---|---|

| | | |
|---|---|---|
| 恶意软件常用权限 | 5/30 | android.permission.CALL_PHONE<br>android.permission.READ_PHONE_STATE<br>android.permission.RECEIVE_SMS<br>android.permission.READ_SMS<br>android.permission.READ_CONTACTS |
| 其它常用权限 | 4/46 | android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS<br>android.permission.FOREGROUND_SERVICE |

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。

## 第三方SDK

| SDK名称 | 开发者 | 描述信息 |
|---|---|---|
| Jetpack Graphics | Google | 利用多个 Android 平台版本中的图形工具降低画面延迟。 |
| 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 ProfileInstaller | Google | 让库能够提前预先编译要由 ART 读取的编译轨迹。 |

## 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。