南明离火
移动应用检测平台

ANDROID 静态分析报告

Paisa • v6.6.2

分析日期: 2024-09-28 05:58:00

应用概览

文件名称:	dev.hemanths.paisa v6.6.2.apk
文件大小:	8.77MB
应用名称:	Paisa
软件包名:	dev.hemanths.paisa
主活动:	dev.hemanths.paisa.MainActivity
版本号:	6.6.2
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	65a14d317ea924ed52cb8918d321bcdb
SHA1:	629143c9cc5e6053850eb71123228a7dcce9b02a
SHA256:	a68599cf0e96c6d81e092bdf4998b1f86909cc376f52320cfe57ee6317858d4f

分析结果严重性

高危	中危	信息	安全	关注
1	7	1	1	1

四大组件信息

Activity组件：4个，其中export的有：0个
Service组件：14个，其中export的有：3个
Receiver组件：17个，其中export的有：4个
Provider组件：1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=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2022-01-05 19:07:22+00:00
有效期至: 2052-01-05 19:07:22+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xe05c7f94b27c4c1dee96b2fed2fcbb685d2c62ef
哈希算法: sha256
证书MD5: 725a67ca0cf85a824b797cc90f820138
证书SHA1: 2ca740d4f3add82c1750c7456889173ebff42e09
证书SHA256: ba1d4a1e8b78c48578470ea226f5301f437daa2bac9ea0e21d0df7774f57c06a
证书SHA512:
328af51740c1c762b0466cd0b0feb9e5b8d3c224a48d7226bc949345a36c4ea75b3cffc2b1e5bb33b2889f4900f7bf511dba09ef8f410e29aa9fd98f47c20a9d

公钥算法: rsa
密钥长度: 4096
指纹: 96410567f4b56a0a420ebb791ca2c3f89bffc7f7c23f78222a75d077d48610a8
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.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.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.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.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
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.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.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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

dev.hemanths.paisa.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.CHECK_LICENSE	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	应用程序已使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **9** | 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存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10、API 29 以接收合其的安全更新。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Broadcast Receiver (dev.hemanths.paisa.glance.PaisaHomeWidgetReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
4	Broadcast Receiver (es.antonborri.home_widget.HomeWidgetBackgroundReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
5	Service (es.antonborri.home_widget.HomeWidgetBackgroundService) 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。

6	Activity设置了TaskAffinity属性 (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	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
7	Service (androidx.glance.appwidget.GlanceRemoteViewsService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_REMOTEVIEWS [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。
8	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。
9	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。
10	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。

</> 安全漏洞检测

高危: **1** | 警告: **6** | 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	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

3	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
4	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
5	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
6	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
7	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
8	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
9	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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。

域名检测

域名	状态	中国境内	位置信息
goo.gle	安全	否	**IP地址:** 67.199.248.12 **国家:** 美利坚合众国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750137 **经度:** -73.997009 **查看:** Google 地图
google.com	安全	否	**IP地址:** 142.250.72.130 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
app-measurement.com	安全	否	**IP地址:** 142.250.72.130 **国家:** 美利坚合众国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
pagead2.googlesyndication.com	安全	否	**IP地址:** 142.250.72.130 **国家:** 美利坚合众国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

goo.gl	安全	否	**IP地址:** 142.250.68.110 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
docs.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures	h3/C1219d.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	A1/b.java
• https://%s/%s/%s	b2/c.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	b2/f.java
• https://github.com/baseflow/flutter-permission-handler/issues	L1/p.java
• https://goo.gle/compose-feedback	Q/AbstractC1471k.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	u2/C1555s.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • https://google.com/search? • https://goo.gle/compose-feedback • https://firebase.google.com/support/privacy/init-options • https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures • https://app-measurement.com/a • https://goo.gl/naoooi • https://app-measurement.com/a • https://%s/%s/%s • https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin • https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings • https://firebase.google.com/support/guides/disable-analytics • www.google.com • https://firebase.google.com/docs/analytics • https://github.com/baseflow/flutter-permission-handler/issues • https://www.google.com	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
Jetpack Glance	Google	Build layouts for remote surfaces using a Jetpack Compose-style API.

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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack Core	Google	Target the latest platform features and APIs while also supporting older devices.
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。

追踪器

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "648a8c15d0a549969[illegible]d61ac[illegible]475bab0"
"google_api_key" : "AIzaSyAgUlvboZ135SrO4OxO44r9NUdze4jwnKs"
"google_crash_reporting_api_key" : "AIzaSyAgUlvboZ135SrO4OxO44r9NUdze4jwnKs"
uh1KHot4xIV4Rw6iJvUwH0N9[illegible]qDiHQ33d09XwGo=
470fa2b4ae81cd56ec[illegible]da9735803434cec591[illegible]
Vn3kj4pUblRGi2[illegible]+OfRRL9nhsaO2uoHQg6[illegible]ExdTE=

GooglePlay应用信息

标题: Paisa - Expense tracker

评分: 3.1584158 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 效率 **Play Store URL:** dev.hemanths.paisa

开发者信息: Hemanth Savarala, 6640674686450056742, Bangalore, India, https://www.hemanths.dev/, monkeycodeapp@gmail.com,

发布日期: 202[illegible]年1月6日 **隐私政策:** Privacy link

关于此应用:

 Paisa - 费用跟踪器：简化您的财务 使用 Paisa 掌控您的资金，Paisa 是专门为您打造的直观的 Material Design 费用跟踪器。通过我们的用户友好界面和强大的功能体验无忧的财务管理。 主要特点 轻松跟踪支出、收入和转账 使用无尽的选项和个性化图标自定义类别 通过动态图表可视化您的支出 按日、

周、月或年过滤交易 □ 获取有关您的财务活动的富有洞察力的摘要 □ 通过简单的备份和恢复选项保护您的数据 □ 为什么选择派萨？ □ 时尚的材质设计：享受现代、干净的界面，使用起来很愉快 □ 用户友好：轻松添加、更新和删除交易 □全面概览：一目了然了解您的消费习惯 □□ 灵活定制：定制应用程序以满足您独特的财务需求 □ 数据安全：确保您的财务信息安全且可访问 □ 持续改进 我们致力于增强您的体验！期待定期更新新功能和改进。 用 □□ 在印度制造 □ 注意：Paisa 正在积极发展。虽然我们力求卓越，但您可能会遇到一些错误或缺少功能。感谢您的耐心和反馈，我们致力于提供最佳的费用跟踪体验。

免责声明及风险提示: