南明离火
移动应用检测平台

ANDROID 静态分析报告

8319.apk

分析日期: 2025-10-14 10:40:52

应用概览

文件名称:	8319.apk
文件大小:	0.6MB
应用名称:	
软件包名:	com.bruce.CBRC.test
主活动:	androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity
版本号:	
最小SDK:	23
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	83542c3c5a2330a7f4cc3d56d75d93a4
SHA1:	4f89ee5d91dbb6d0d29d380fe981fa0a4[illegible]ea34c
SHA256:	4bfa72d7fd9cf52331ffc389bb488[illegible]b20507a391ffa2051de99e731c093906f

分析结果严重性分布

高危	警告	信息	安全	关注
2	5	1	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有：2个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：0个，其中export的有：0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True

v3 签名: False
v4 签名: False
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-21 06:14:05+00:00
有效期至: 2055-08-14 06:14:05+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha256
证书MD5: ecf2a064ab95990f4e35cfd745e41c69
证书SHA1: 2167c8219b199c6ea809801412b3384a10c97573
证书SHA256: ac023ded43a0e17a09c8776166697e63b7da7cebf9c116cfeba63df173aac50c
证书SHA512:
11484dd58a6024ea3cd3b13675bdb1a60003323feac0d79dc631cdd34a66d440f484bc951199880d3376bca311a44476011bdd607105d2eb733bf368f1603073

公钥算法: rsa
密钥长度: 2048
指纹: 1d502be137a3c9b04fc03a18e34e17c49438e4f4d96d6ec1a83cf41c40d36610
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.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。

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: **1** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。
检测到调试证书签名	高危	检测到应用使用调试证书签名。请勿在生产环境中使用调试证书。

Manifest 配置安全分析

高危: **1** | 警告: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用可被调试 [android:debuggable=true]	高危	应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。
2	应用数据存在泄露风险 未设置 [android:allowBackup] 标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。

3	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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。

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
3	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

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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	2/46	android.permission.REORDER_TASKS

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 组件分析

SDK名称	开发者	描述信息
Jetpack Test	Google	在 Android 中进行测试。

免责声明及风险提示: