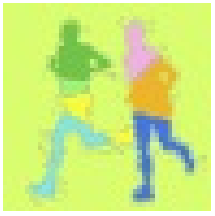
南明离火
移动应用检测平台

ANDROID 静态分析报告



Krun • v1.0

分析日期: 2025-07-05 13:51:34

应用概览

文件名称:	Krun.apk
文件大小:	21.99MB
应用名称:	Krun
软件包名:	com.example.test1
主活动:	com.example.test1.MainActivity
版本号:	1.0
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：安全
MD5:	937e13ed595c1b215b57683f46ec0ca8
SHA1:	3f08b9e2aa388e230473abbd7bb19111fced8c11
SHA256:	eaf3dd76940cf0f42ed16d1b4d728ef1a787ce707ed4efafb6d8da3ff5a66190

分析结果严重性分布

高危	中危	信息	安全	关注
2	3	2	1	0

四大组件导出状态统计

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

应用签名证书信息

APK已签名
v1 签名: False
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: 2023-08-18 02:38:16+00:00
有效期至: 2053-08-10 02:38:16+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha256
证书MD5: bb52bc1ba39f16bcf7bc97840b17403d
证书SHA1: 29f6905a2201d00f12a90f91cc57449105483d28
证书SHA256: 2bb07a1286d7ec312b95ac19ffa767512a00c8c41be56cc4fd2e489cd685713f
证书SHA512:
cbada8efe371286292c2265635928c1eb872a7567dff2857a8c8127c7aefa5139356300f5eca238894a09c612ca17c50f2f395c8c8504e5[illegible]ddda6d54c1bfc

公钥算法: rsa
密钥长度: 2048
指纹: 4a8885d022a0be08fc11381c3097efdbaac7976b0c61abd2da44c2c01771539e
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
com.example.test1.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: **0** | 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: **2** | 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	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **1** | 信息: **2** | 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	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	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	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	6/46	

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.zetetic.net	安全	否	**IP地址:** 13.227.74.64 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/sqlcipher/android-database-sqlcipher • https://www.zetetic.net/sqlcipher/ • https://www.zetetic.net/sqlcipher/license/	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以便提供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	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

敏感凭证泄露检测

可能的密钥
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

免责声明及风险提示:

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。