



ANDROID 静态分析报告



CClauncher • v9.1.5

分析日期: 2025-07-07 09:25:59

i应用概览

文件名称:	CCLauncher vv9.1.5.apk
文件大小:	3.5MB
应用名称:	CCLauncher
软件包名:	app.cclauncher
主活动:	app.cclauncher.MainActivity
版本号:	9.1.5
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:	64/100 (低风险)
杀软检测:	经检测, 该文件安全
MD5:	5695f9105985942141cd6619f9f16eba
SHA1:	7583c45c2f135a3b13cd62777bff79af9f7c683d
SHA256:	0f1687d9c3ec0c87bb37c183b766a1d3711e667bb3c85aa27e287c0c42596a

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	1	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: 5个, 其中export的有: 1个
Receiver组件: 9个, 其中export的有: 2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: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa_pkcs1v15

有效期自: 2024-11-16 14:41:35+00:00

有效期至: 2052-04-03 14:41:35+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

序列号: 0x38dcf17bac9ffd69

哈希算法: sha384

证书MD5: a3d2c2ca563b856d7bdc8e83c13eda44

证书SHA1: e458ef8d3b8fa4d25f672a8ae744fc96edacd33f

证书SHA256: 57f73d58f4049f378ba988eae6edd1cc8cd245e0647e0f83dd669c450f4d056e

证书SHA512: 742a65c2d65ac29e5675d36ce44d3a8cd01c6865251b7a84f16f6646c37cc10b20fe8f2f7d57b15598891554fc56e653df5e61deff4b7e2537d5b9916386fed5

公钥算法: rsa

密钥长度: 3072

指纹: 42597d2f8f81a1babafbce06c509c1177e4bda3803cf790dd30ed64423c3a6b1

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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
android.permission.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
android.permission.BIND_APPWIDGET	签名(系统)	选择窗口小部件	允许应用程序告诉系统哪个应用程序可以使用哪些窗口小部件。具有该权限的应用程序可以允许其他应用程序访问个人数据。普通应用程序不能使用此权限
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_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.RECEIVE_BOOT_COMPLETE	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）
app.clauncher.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: 0 | 警告: 0 | 信息: 1

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

🔍 Manifest 配置安全分析

高危: 0 | 警告: 4 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 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。
3	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

4	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: 0 | 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-STORE-3	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	3/30	android.permission.SET_WALLPAPER android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	3/46	android.permission.BIND_APPWIDGET android.permission.ACCESS_NETWORK_STATE 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 组件分析

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。
Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。DataStore 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
Jetpack App Startup	Google	App Startup 库提供了一种直接、高效的方法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。

Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成