南明离火
移动应用检测平台

ANDROID 静态分析报告

Exo Light - v1.0.3

分析日期: 2025-08-04 11:56:57

应用概览

文件名称:	Exo Light v1.0.3.apk
文件大小:	11.67MB
应用名称:	Exo Light
软件包名:	com.niresh23.fanlightcontroller
主活动:	com.niresh23.fanlightcontroller.MainActivity
版本号:	1.0.3
最小SDK:	28
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:	0ad6393ea8bff737b6130b9e556fbba1
SHA1:	76d8c6fbb13ee5d20c4e9fba1be03205ef544a7
SHA256:	65acdd69c5ef24532d9a34fcb86d3c9920b6da0cb7489c94028d038ea9a0b6

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：2个，其中export的有： 0个
Service组件：1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: False
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: 2024-03-31 17:46:45+00:00
有效期至: 2054-03-31 17:46:45+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xdfae5ed0edd8dbb5b72caabfd719980c604455f5
哈希算法: sha256
证书MD5: 2a8c4d1197174773437017c0e3c9bf21
证书SHA1: cc27f8fee5a1f02dc1fddedffe5db6a4d487f847
证书SHA256: b30160be9ac6cfe4669ecf7275f947389d7b55c70ec0512b5ad95221717d7122
证书SHA512:
bfd6ce06c38cbc5276f990163b14a6b720622711353c59a9e8c1b27f94ba65d409e80b5b4bd5a1faf067a10c9440f33e1267fae64204c91021e9103d54aec44e

公钥算法: rsa
密钥长度: 4096
指纹: 0428865fb852b41511f39549a6450b04ffad7c9a0a045096276ccb65f3f911c1
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.FOREGROUND_SERVICE_MICROPHONE	普通	允许使用麦克风的前台服务	允许常规应用程序使用类型为“麦克风”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	普通	通过连接的设备使用启用前台服务	允许常规应用程序使用类型为“connectedDevice”的 Service.startForeground。

com.niresh23.fanlightcontroller.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: **2** | 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	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: **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	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

本报告由南明离火移动安全分析平台生成

应用行为分析

编号	行为	标签	文件
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	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	2/30	android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	3/46	android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN 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
Dexter	Karumi	Dexter 是一个 Android 库，它简化了运行时请求权限的过程。
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
8ec91001-f315-4f60-9fb8-838830daea50

8ec91002-f315-4f60-9fb8-838830daea50

Google Play 应用市场信息

标题: Exo Light

评分: 3.8888888 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.niresh23.fanlightcontroller

开发者信息: Reshetov Ink., 5766459820662925965, None, None, niksama3@gmail.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

应用程序允许用户连接他们的 EXO 荧光棒版本。 3、改变颜色并使用音频可视化工具。

免责声明及风险提示: