南明离火
移动应用检测平台

ANDROID 静态分析报告

RADIO CATARAY • v4.0

分析日期: 2025-07-07 16:34:31

应用概览

文件名称:	RADIO CATARAY v4.0.apk
文件大小:	13.7MB
应用名称:	RADIO CATARAY
软件包名:	streamingpro.cat
主活动:	com.sekhontech.singlestationapp.SplashActivity
版本号:	4.0
最小SDK:	26
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:	55/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	62fb9a920e5526c1b28373d02cd18e37
SHA1:	c658e799491fbeb91cacfa151cdb3826938ad7bd
SHA256:	db4459b2eadd9abfb96555f1036ac44[illegible]34f566300b467a91a8e887b7fd4e3b20

分析结果严重性分布

高危	中危	信息	安全	关注
0	11	2	1	1

四大组件导出状态统计

Activity组件：7个，其中export的有：2个
Service组件：14个，其中export的有：1个
Receiver组件：11个，其中export的有：2个
Provider组件：4个，其中export的有：0个

本报告由南明离火移动安全分析平台生成

应用签名证书信息

APK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: 2022-03-28 23:20:57+00:00
有效期至: 2052-03-28 23:20:57+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xbfa8a7b9f87c2a6a0b3a0483acafe87d669e017
哈希算法: sha256
证书MD5: 0dd59b3448c831a21bce0a5daf55a9ed
证书SHA1: 174c3037cdca0d91df2cb668046bc37439cae3c7
证书SHA256: 769c23cf8aa7020f6d9567bdda81d0a3218e7a2486cae49e21e3cb614ea56402
证书SHA512:
7c4a083d231b5e461e878ca7234a75ce6a12516f08abd53d6834d3a682f4ce10cb212c91a5893279741121a322aecdd8a7bc242e385b8[illegible]9f75118d5cd3195

公钥算法: rsa
密钥长度: 4096
指纹: 8d4c46e996ff3cecd306390190a4f8f7eb98ac4783c4262677a19693c3269ed6
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.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.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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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。
streaming.pix.cat.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: **7** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
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	Activity (com.sekhontech.singlestationapp.MainActivity) 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 (com.sekhontech.singlestationapp.TvActivity) 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。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
6	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。

本报告由南明离火移动安全分析平台生成

7	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。

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	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-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
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
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00051	通过setData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
00056	修改语音音量	控制	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	1/30	android.permission.WAKE_LOCK

其它常用权限	6/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
radio-ding.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
streaminghd.es	安全	否	**IP地址:** 104.21.26.97 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
itunes.apple.com	安全	是	**IP地址:** 49.71.74.25 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
wa.me	安全	否	**IP地址:** 31.13.70.49 **国家:** 美国 **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

URL 链接安全分析

URL信息	源码文件

• https://www.facebook.com/ • https://play.google.com/store/apps/details?id= • https://wa.me/ • https://itunes.apple.com/search?media=music&limit=1&term=	com/sekhontech/singlestationapp/MainActivity.java
• https://streaminghd.es/apis/api.php?	com/sekhontech/singlestationapp/Constant.java
• https://radio-ding.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://radio-ding.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/586046562565/namespaces/firebase:fetch?key=AIzaSyCJaJITtS[illegible]RcxDBnjmneR1iBxSNxe[illegible]bh[illegible]E ） 已禁用。响应内容如下所示：
		
		{
		  "state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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 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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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。

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/3[illegible]
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "@7F12001[illegible]"
"app_id" : "ca-app-pub-9409505951509524~1299125694"
"firebase_database_url" : "https://radio-ding.firebaseio.com"
"google_api_key" : "AIzaSyCJaJITtSaRcxDBnjmneR1iBxSNxeYbh[illegible]"
"google_app_id" : "1:586046562565:android:b4257f303e831[illegible]c5"
"google_crash_reporting_api_key" : "AIzaSyCJaJITtSaRcxDBnjmneR1iBxSNxeYbhcE"

Google Play 应用市场信息

标题: RADIO CATARAY

评分: 4.875 **安装:** 100+ **价格:** 0 **Android版本支持:** **分类:** 娱乐 **Play Store URL:** streamingpro.cat

开发者信息: StreamingPRO, StreamingPRO, None, https://streamingchilenos.cl, contacto@streamingchilenos.cl,

发布日期: 2022年3月28日 **隐私政策:** Privacy link

关于此应用:

Radio Cataray 的创建是为了在您的日常生活中以愉快的节目陪伴您，让您忘记一点日常琐事。 伴随着现代音乐和回忆，伴随着对智利的问候，不要忘记我们的民间传说，伴随着我们演员团队创作的幽默节目，以及我们将通过广播每天添加的无穷无尽的新闻。

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

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。