南明离火
移动应用检测平台

ANDROID 静态分析报告

Android System • v14

分析日期: 2025-07-05 13:47:11

应用概览

文件名称:	AdExtServicesApk.apk
文件大小:	11.55MB
应用名称:	Android System
软件包名:	com.android.ext.adservices.api
主活动:	not_found_main_activity!!
版本号:	14
最小SDK:	30
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:	56/100 (中风险)
杀软检测:	AI评估：安全
MD5:	1b9badec7fb7ff45a3741444dbcf26e2
SHA1:	8e452399f8cecc80872f7cb772f3960ec0105fb6
SHA256:	e7ba83ab96ced48287c71f181bd0c839cc03fe30553be160067d864e0b3f4d8

分析结果严重性分布

高危	中危	信息	安全	关注
0	21	1	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 7个
Service组件：24个，其中export的有： 7个
Receiver组件：3个，其中export的有： 3个
Provider组件：3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=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2022-02-24 16:05:47+00:00
有效期至: 2049-07-12 16:05:47+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x7ddc5ba360c0bf605c37f568555ebf8babf0c80b
哈希算法: sha256
证书MD5: a38e078fe09c1d48ff1d7918a0bf7510
证书SHA1: 85e21f423dc05572b222354f6d9645789141e5ed
证书SHA256: ccc51124be4ab8f81bca7d32f6b3eb1ae04770e5ddfcc73a0108e1f94ec9f5f2
证书SHA512:
8d772266d820ba8d49b2f8eb4d53031306a7c3f83046adddbae6ee0dece824042311a3e861f66aee5ab03d16dcbacf39c79cb209de0ab17e9075096b0fc11419

公钥算法: rsa
密钥长度: 2048
指纹: 25a9bb3a2d93891bb1dca38eb33fb17f0e617289bd019d077237a5c8911d3b06
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.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.READ_DEVICE_CONFIG	未知	未知权限	来自 android 引用的未知权限。
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.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.ACCESS_ADSERVICES_MANAGER	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_PRIVILEGED_AD_ID	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_PRIVILEGED_APP_SET_ID	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_BOOT_COMPLETED	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。
com.android.ext.adservices.api.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: **17** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.android.adservices.ui.settings.activities.AdServicesSettingsMainActivity) 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。
2	Activity (com.android.adservices.ui.settings.activities.TopicsActivity) 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。
3	Activity (com.android.adservices.ui.settings.activities.BlockedTopicsActivity) 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.android.adservices.ui.settings.activities.AppsActivity) 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	Activity (com.android.adservices.ui.settings.activities.BlockedAppsActivity) 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。
6	Activity (com.android.adservices.ui.settings.activities.MeasurementActivity) 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。
7	Activity (com.android.adservices.ui.notifications.ConsentNotificationActivity) 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。
8	Service (com.android.adservices.adselection.AdSelectionService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。

9	Service (com.android.adservices.customaudience.CustomAudienceService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
10	Service (com.android.adservices.topics.TopicsService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
11	Service (com.android.adservices.adid.AdIdService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
12	Service (com.android.adservices.appsetid.AppSetIdService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
13	Service (com.android.adservices.measurement.MeasurementService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
14	Service (com.android.adservices.common.AdServicesCommonService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
15	Broadcast Receiver (com.android.adservices.service.common.AdExtBootCompletedReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.INIT_EXT_SERVICES [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。
16	Broadcast Receiver (com.android.adservices.service.common.PackageChangedReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
17	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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
4	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
5	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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.RECEIVE_BOOT_COMPLETED
其它常用权限	2/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE

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

本报告由南明离火移动安全分析平台生成

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 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。

敏感凭证泄露检测

可能的密钥
301aa3cb081134501c45f1422abc66c24224fd5ded5fdc8f17e697176fd866aa
4d9d365c6c901ca8a91490ed484cc0b8
c01fb00f9478984f9974c146f3255d17
c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
89f92685b48a7473e27a458112ea8722
49b88ce6275a012c1c9517982d7d19e7
7776c9d31bbe12a578e7a4210c71380a
e8077f0304bb6f00f99da1b5a1c9236e
6c8694d56711b3a5a84445add2443b15
56d0cab85f8ecced8ce9ac6403442fd7
d2e49728d938d87d4313c08939b2dd5a
686d5c450e00ebe600f979300a29234544ea4de42f24ede07a073f2bc6b94a3a2
3d7d3d0f6c1d3f5d6350ed5d31a1f669
a40da80a59d170caa950cf15c18c454d47a39b26989d8b40ecd745ba71bf5dc
6cecc50e34ae31fb5d78986d6d6d3736c571ded2f2459527793e1f054eb0c9b

免责声明及风险提示: