南明离火
移动应用检测平台

ANDROID 静态分析报告

Smart Unit Converter，v3.0.0

分析日期: 2025-03-11 08:42:56

应用概览

文件名称:	21cbe65296bbf3fcd24db3c4bf412a1221f1125eab843d6e1fec3d1c77ad3ad9.apk
文件大小:	4.57MB
应用名称:	Smart Unit Converter
软件包名:	com.converter.unitconverter
主活动:	com.converter.unitconverter.MainActivity
版本号:	3.0.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	64/100 (低风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	3c33237d40cbac5f370cb41654d0029e
SHA1:	95f9c15917af1cd76b96e5864ffbfaf5ff8ebfd
SHA256:	21cbe65296bbf3fcd24db3c4bf412a1221f1125eab843d6e1fec3d1c77ad3ad9

分析结果严重性

高危	中危	信息	安全	关注
0	8	2	2	1

四大组件信息

Activity组件：6个，其中export的有： 0个
Service组件：6个，其中export的有： 1个
Receiver组件：3个，其中export的有： 1个
Provider组件：5个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=91, ST=Gujrat, L=Ahmedabad, O=Sathwara Infotech, OU=Sathwara Infotech, CN=Bhavesh Sathwara
签名算法: rsassa_pkcs1v15
有效期自: 2018-08-24 17:33:38+00:00
有效期至: 2118-07-31 17:33:38+00:00
发行人: C=91, ST=Gujrat, L=Ahmedabad, O=Sathwara Infotech, OU=Sathwara Infotech, CN=Bhavesh Sathwara
序列号: 0x214b35eb
哈希算法: sha256
证书MD5: df7fbabe1a7d8554d555023ac3a4c09f
证书SHA1: d41684922dbea177cc1446cb8039c36aa8a720fe
证书SHA256: 7ec989bcc7c20f1a575772d64d5b22fa7c5b3a585fd3db1a43d9b883f5b9fa32
证书SHA512:
3ff77e5d40c19ad62d6a0b3a711080d8fefba2675f00c806e324ee7eede6b1d99f028053a7bd79624ef926de0f344d4a306d1803bdccaf7909b9d91f707479

公钥算法: rsa
密钥长度: 2048
指纹: 64bd9ab49de9e7a8d171fe611a2aad8eb960037c356f0a954df3fb99283591bf
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
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_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
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。
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	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）

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

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

序号	问题	严重程度	描述信息
1	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
2	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
3	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

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	MD5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
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

4	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
5	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MST G-RESILIENCE-1	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	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
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限

敏感权限分析

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	7/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID 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。

域名检测

域名	状态	中国境内	位置信息
smartunitconverter-46f3c.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **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
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
goo.gl	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id=	v3/d.java
• https://plus.google.com/	k2/i1.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	n1/b.java
• https://fundingchoicesmessages.google.com/a/consent	w2/g2.java
• https://goo.gl/j1swqy	x2/s0.java
• www.google.com	q1/s.java

• https://play.google.com/store/apps/details?id=	u3/a.java
• https://smartunitconverter-46f3c.firebaseio.com	自研引擎-S

FIREBASE数据库分析

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://smartunitconverter-46f3c.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/296463719121/namespaces/firebase:fetch?key=AIzaSyAdKXtz1TguwTfDBcNfivzvKYqz1y1ZIko ）已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

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。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 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。

追踪器

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

密钥凭证

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-7164217328635358~4326209548"
"firebase_database_url" : "https://smartunitconverter-46f3c.firebaseio.com"
"google_api_key" : "AIzaSyAdKXtz1TguwTfDBcNfivzvKYqzcy12Iko"
"google_app_id" : "1:296463719121:android:6d424487bda7a83b1643f0"
"google_crash_reporting_api_key" : "AIzaSyAdKXtz1TguwTfDBcNfivzvKYqzcy12Iko"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
B3EEABB8EE11C2BE770B684D95219ECB

GooglePlay应用信息

标题: Smart Unit Converter

评分: 4.319149 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.converter.unitconverter

开发者信息: Sathwara InfoTech, 6608251630327988574, 415, Akshar Arcade, New India Colony Rd, nr. Devasya International School, Naroda, New India Colony, Nikol, Ahmedabad, Gujarat 382345, http://sathwarainfotech.com, sathwarainfotech@gmail.com,

发布日期: 2018年8月24日 **隐私政策:** Privacy link

关于此应用:

- 货币（美元、加元、英镑、比索等） - 温度（摄氏度、华氏度、开尔文等） - 长度（公里、英里、米、码、英尺等） - 质量/重量（公斤、磅、盎司、吨、石头等） - 速度（公里/小时、英里/小时、节等） - 面积（平方公里、平方英里、公顷、英亩等） - 烹饪（茶匙、汤匙、杯子、品脱、夸脱、盎司等） - 体积（立方米、立方英寸、升、加仑等） - 压力（千帕、巴、PSI 等） - 功率（瓦特、千瓦、马力等） - 能量（焦耳、卡路里、BTU 等） - 时间（年、月、日、小时、秒等） - 油耗（每加仑英里数、每 100 公里升数等） - 数字存储（位、字节、兆字节、千兆字节等）

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，深入扫描软件中中潜在的漏洞和安全隐隐患。