



ANDROID 静态分析报告



Ampture v4.3.1

分析日期: 2025-08-28 18:33:13

i应用概览

文件名称:	Ampture v4.3.1.apk
文件大小:	15.63MB
应用名称:	Ampture
软件包名:	com.kaunik.ampture
主活动:	com.kaunik.ampture.activity.SplashActivity
版本号:	4.3.1
最小SDK:	21
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:	47/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	8c7f0b0fd0934aab3408e46d64780bf5
SHA1:	ca162fa904cb347a2948b0f441d940c8bee651c7
SHA256:	c046d51efe7f7a8d0bb73a54ca078627a4e98afabd3cd030c0bdb95bc030dff

分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
2	8	2	1	0

四大组件导出状态统计

Activity组件: 15个, 其中export的有: 1个
Service组件: 4个, 其中export的有: 0个
Receiver组件: 4个, 其中export的有: 3个
Provider组件: 2个, 其中export的有: 0个

应用签名证书信息

APK已签名

v1 签名: True

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: 2023-10-24 11:31:57+00:00

有效期至: 2053-10-24 11:31:57+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0xd9dfbe9029f29950adb447051ef11d4a11e74d87

哈希算法: sha256

证书MD5: 4ed0041e26332b049a76d1e3915b0fde

证书SHA1: 14fbea41c89ac766c00688a97c2b6800eda20d8c

证书SHA256: f272a5d30bb91c37f4f6093f7295e12ecac00719bfa87e5d3e582570f4387c43

证书SHA512: b16214318c79131a1d828d8da0dc415e5063dcbc7ec8b49219801af70544753a698bb6fe056bc5a6b2d6fa798c1770bd2b537ed85cb5cf9c27648f1b2d05a8c17

公钥算法: rsa

密钥长度: 4096

指纹: b2a3337ffe62043c343074605e9d74f29997c5483d1884eeff70a25eb87e841c

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.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.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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
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.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.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。
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.kaunik.ampture.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
----------	--------

com.kaunik.ampture.activity.MainActivity	Schemes: http://, https://,
--	-----------------------------

🔒 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: 1 | 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: 5 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurity Config=@7F160004]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
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.kaunik.ampt ure.activity.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	Broadcast Receiver (com.k aunik.ampture.activity.Am ptureAppWidget) 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。
5	Broadcast Receiver (com.g oogle.firebase.iid.Firebase InstanceIdReceiver) 受权 限保护，但应检查权限保护 级别。 Permission: com.google.a ndroid.permission.S END [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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 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: 2 | 警告: 1 | 信息: 2 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	此应用程序将数据复制到剪贴板。 敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员: 解锁高级权限
2	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当 ('跨站脚本') OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员: 解锁高级权限
3	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
4	不安全的Web视图实现。可能允许在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员: 解锁高级权限
5	已启用WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员: 解锁高级权限

应用行为分析

编号	行为	标签	文件
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

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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	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.VIBRATE android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE

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
vividview.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
www.perplexity.ai	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
ampturetodolist.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图

kweather.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
ampturecurrencyconverter.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
ampturelanguagetranslate.netlify.app	安全	否	IP地址: 52.52.192.191 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
www.bing.com	安全	否	IP地址: 22.60.173.17 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
silver-sprinkles-aa6f40.netlify.app	安全	否	IP地址: 13.52.188.95 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
qrampture.netlify.app	安全	否	IP地址: 13.52.188.95 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
duckduckgo.com	安全	否	IP地址: 52.250.42.157 国家: 美国 地区: 华盛顿 城市: 昆西 纬度: 47.234463 经度: -119.852577 查看: Google 地图

amptureurlshortner.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
ampturecalculator.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
ampture.xyz	安全	否	IP地址: 150.05.255.38 国家: 日本 地区: 东京 城市: 东京 纬度: 35.689499 经度: 139.692327 查看: Google 地图
search.yahoo.com	安全	否	IP地址: 98.136.144.138 国家: 美国 地区: 华盛顿 城市: 昆西 纬度: 47.2342997 经度: -119.8525504 查看: Google 地图
65c0bdac12f87a00764c4ba6--resonant-narwhal-b289eb.netlify.app	安全	否	IP地址: 104.18.26.48 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
- https://docs.google.com/document/d/1hsb19rlie3xyc7pfz0khllaihfd4mziyham3xulozb0/edit?usp=sharing - https://ampture.xyz - https://play.google.com/store/apps/details?id=com.kaunik.ampture - http://play.google.com/store/apps/details?id= - https://docs.google.com/document/d/1xqomcsrn7e7cshezoexhzwkok36pirptt47uo-4pmy/edit?usp=sharing - https://docs.google.com/document/d/1b9hdwj0yhg5l-khbyjygmglrpf0fnrmt56onkcmzkk0/edit?usp=sharing	com/kaunik/ampture/activity/mSetting sActivity.java
https://www.google.com	com/kaunik/ampture/activity/TabsBott omSheet.java

- https://ampturetodolist.netlify.app - https://qrampture.netlify.app - https://65c0bdac12f87a00764c4ba6--resonant-narwhal-b289e3.netlify.app - https://silver-sprinkles-aa6f40.netlify.app - https://ampturecalculator.netlify.app - https://vividview.netlify.app - https://ampturelanguagetranslate.netlify.app - https://amptureurlshortner.netlify.app - https://kweather.netlify.app - https://ampturecurrencyconverter.netlify.app	com/kaunik/ampture/activity/ExploreActivity.java
- https://www.bing.com/search?q= - https://search.yahoo.com/search?p= - https://www.perplexity.ai/search?q= - https://duckduckgo.com/?q= - https://www.google.com/search?q=	com/kaunik/ampture/fragment/BrowseFragmen.java

🔌 Firebase 配置安全检测

标题	严重程度	描述信息
Firebase远程配置已禁用	安全	Firebase远程配置URL (https://firebase.remoteconfig.googleapis.com/v1/projects/709595178168/namespaces/firebase:fetch?key=AIzaSyBUdCFp78UJ307uv8WtH1emVc2JzUiK47s) 已禁用。响应内容如下所示： <pre>{ "state": "NO_TEMPLATE" }</pre>

📦 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。
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 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).

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
contact.kaunik@gmail.com	com/kaunik/ampture/activity/mSettingsActivity.java

🕵 第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

🔑 敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyBUuCFp78UJ307uv8WHI1emVC2jzUiK47s"
"google_app_id" : "1:709595178168:android:d5afcb53d40dc82244404d"
"google_crash_reporting_api_key" : "AIzaSyBUuCFp78UJ307uv8WHI1emVC2jzUiK47s"
65c0bdac12f87a00764c4ba6--
kHBYjYGMgxIRp0FnrmT56ONKcmzkk0/edit

▶ Google Play 应用市场信息

标题: Ampture Browser: Fast & Secure

评分: 4.0540543 安装: 1,000+ 价格: 0 Android 版本支持: 分类: 工具 Play Store URL: [com.kaunik.ampture](https://play.google.com/store/apps/details?id=com.kaunik.ampture)

开发者信息: Kaunik, 6281444463423838746, None, None, contact.kaunik@gmail.com,

发布日期: 2023年10月24日 隐私政策: [Privacy link](#)

关于此应用:

Ampture 浏览器: 安全、快速、轻型 Web 浏览器 Ampture Web 浏览器是一款快速、安全、智能的移动浏览器; 它专为手机、平板电脑和 Chromebook 设计。适用于 Android 的 Ampture Web 浏览器是一款快速、功能齐全、安全、轻量级且智能的 Android 移动浏览器; 最值得信赖的隐私浏览器之一。Ampture Web 浏览器使您能够重新掌控您的 Web 体验。使用 Ampture 浏览器扩大您的网络 适用于 Android 的 Ampture Web 浏览器主要功能: - Web Explorer: 超轻量级 - 上网速度加速 - Web Explorer: 安全浏览 - 隐身浏览。私密浏览网页, 不保存任何网页浏览历史记录 - 网页主页快速拨号 - 个性化书签 - 轻松保存您喜爱的网站 - 网页浏览器: 文本搜索 - 网络浏览器具有简单、干净且易于使用的用户界面 - 网络互联网快速启动, 快速加载和渲染页面 - 网络互联网多点触控捏缩放 - 网络浏览器支持菜单中的全屏选项 - 轻松添加书签 - 网络互联网可以隐藏设置中的放大/缩小按钮 - Web 支持下载管理器、查看图像、保存图像 - 网络互联网: 新主页、谷歌页面 - 通过重新加载页面观看没有广告的视频 (例如在 YouTube 上) - 将网页另存为任意尺寸的 PDF (例如 A4、A5) - 缩放和搜索任何网页 - 禁用 JavaScript 和不需要的 cookie, 以获得更多隐私 - 全屏浏览并隐藏状态栏 - 使用专用的前进按钮、书签和隐身功能 - 在后台打开选项卡并访问桌面站点 - 使用数据保护模式来减少数据使用 - 它还为您提供方便的工具, 例如: 单位转换器、壁纸、天气、语言翻译、二维码生成器、tts 转换器、货币转换器 - 触觉反馈和漂亮的用户友好的用户界面 - 更改搜索引擎选项 - 安全浏览模式 - 有用的功能, 例如: 在页面上查找、转到顶部、调整字体大小、网页缩放 - 为您的浏览器定制背景壁纸 - 在应用程序快捷方式中打开网站 - 阻止自动下载和增强的隐私模式 以及更多! 更多精彩功能, 欢迎下载体验! 它是在 Wi-Fi、4G 和 5G 等快速网络连接上使用的理想 Web 浏览器。它旨在让您的 Android 设备更有效、更轻松地连接网络!

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患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成