南明离火
移动应用检测平台

ANDROID 静态分析报告

Cleaner for WhatsApp • v2.9.6

分析日期: 2025-10-12 16:28:11

应用概览

文件名称:	2d03c86040a86f21386ce29a9ea9f24aceb2ebc3f4141bcef686347b6b9af59c.apk
文件大小:	13.32MB
应用名称:	Cleaner for WhatsApp
软件包名:	com.lookandfeel.cleanerforwhatsapp
主活动:	com.lookandfeel.cleanerforwhatsapp.SplashscreenActivity
版本号:	2.9.6
最小SDK:	21
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:	54/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	ce1e693fedb3c7df3ced45983a526796
SHA1:	50d321c7496b948a0108f5[illegible]83c8e37a7517f3b79
SHA256:	2d03c86040a86f21386ce29a9ea9f24aceb2ebc3f4141bcef686347b6b9af59c

分析结果严重性分布

高危	中危	信息	安全	关注
0	16	2	1	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 1个
Service组件：13个，其中export的有： 1个
Receiver组件：12个，其中export的有： 3个
Provider组件：5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: 2017-09-04 17:19:33+00:00
有效期至: 2047-09-04 17:19:33+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x75d9b2f308085bd6e3925bf223c127573138f88f
哈希算法: sha256
证书MD5: c27cbb3cd2ea147315f23f1d0f52f68e
证书SHA1: 3e43cf70cd134f3da2a3c4b85e739912f85fe619
证书SHA256: 8430d7330dfd719051d0167c5a37873ba3606ebf6438fe842050aa70a87df25f
证书SHA512:
8c06e941c4f440a494d1706e19ea055ff574a933558cbe066365e3dfc3dc1feb0bc13c128453406eb0fd9d9867249591ae13b03051e53943cae49efcd0acc7f0

公钥算法: rsa
密钥长度: 4096
指纹: 1fa6b2d464ce81f62395342e3150a781fc9c1d068d9587eea6cf0cf30c2b551d
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.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.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_INTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.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。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。

android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
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。
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）
com.lookandfeel.cleanerforwhatsapp.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: **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: **6** | 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	Activity (com.lookandfeel.cleanerforwhatsapp.shareit.ShareApp) 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	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。

4	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。
5	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。
6	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: **7** | 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	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
3	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
4	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	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

6	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
7	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
8	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
9	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

应用行为分析

编号	行为	标签	文件
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
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
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
00013	读取文件并将其放入流中	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
00091	从广播中检索数据	信息收集	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
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	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
00094	连接到 URL 并从中读取数据	命令 网络	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
00012	读取数据并放入缓冲流	文件	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.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	8/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET 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 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
googlemobileadssdk.page.link	安全	否	**IP地址:** 172.217.168.193 **国家:** 瑞士 **地区:** 苏黎世 **城市:** 苏黎世 **纬度:** 47.366825 **经度:** 8.549790 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 220.181.174.166 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 220.181.174.162 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
wpcleaner.lookfeel.me	安全	否	**IP地址:** 87.98.231.3 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
cleanerforwhatsapp.blogspot.com	安全	否	**IP地址:** 142.251.36.33 **国家:** 德国 **地区:** 拜仁 **城市:** 慕尼黑 **纬度:** 48.137428 **经度:** 11.575490 **查看:** Google 地图

cleaner-for-whatsapp-21f5c.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

URL 链接安全分析

URL信息	源码文件
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	M3/C0448x.java
• https://googlemobileadssdk.page.link/admob-android-update-manifest • https://googlemobileadssdk.page.link/ad-manager-android-update-manifest	G1/C0238p1.java
• http://cleanerforwhatsapp.blogspot.com/2018/06/privacy-policy.html • https://play.google.com/store/account/subscriptions?sku= • https://play.google.com/store/apps/dev?id=6324983890747629651	com/lookandfeel/cleanerforwhatsapp/MainActivity.java
• http://play.google.com/store/apps/details?id=	com/lookandfeel/cleanerforwhatsapp/shared/N.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	M3/C5647x.java
• https://%s/%s/%s	i3/c.java
• www.google.com	F1/t.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c1/b.java
• https://wpcleaner.lookfeel.me/checkpurchasedata.php	com/lookandfeel/cleanerforwhatsapp/SplashscreenActivity.java
• https://googlemobileadssdk.page.link/admob-android-update-manifest • https://googlemobileadssdk.page.link/ad-manager-android-update-manifest	G1/C0374p1.java
• https://wpcleaner.lookfeel.me/setpurchasedata.php	com/lookandfeel/cleanerforwhatsapp/PremiumActivity.java
• http://cleanerforwhatsapp.blogspot.com/2018/06/privacy-policy.html	com/lookandfeel/cleanerforwhatsapp/SettingsActivity.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	U3/g.java
• https://play.google.com/store/apps/details?id=%1$s • https://cleaner-for-whatsapp-21f5c.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://cleaner-for-whatsapp-21f5c.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/356385950856/namespaces/firebase:fetch?key=AIzaSyBlFhRrQruJb_vOGLDSHXSq8sIlc2mYgdk ） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		
		{
		"entries": {
		"interstitial_caps": "3"
		},
		"state": "UPDATE",
		"templateVersion": "41"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
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 的形式发布自动平台更新。 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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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 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/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
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" : "ca-app-pub-9786990800777347~7846656239"
"com.google.firebase.crashlytics.mapping_file_id" : "c476973e5c204e8fac5a7ef1fdcfd79d"
"firebase_database_url" : "https://cleaner-for-whatsapp-21f5c.firebaseio.com"
"google_api_key" : "AIzaSyBlFhRrQruJb_vOGLDSHXSq8sIlc2mYgdk"
"google_app_id" : "1:356385950856:android:84bd0a6476e8c429"
"google_crash_reporting_api_key" : "AIzaSyBlFhRrQruJb_vOGLDSHXSq8sIlc2mYgdk"
4D2FFAC1A1EF2A2CEB27EAFAA7A96AB9
cbb38b64663f7dff79377e88d383699d
2ac82133871e7e928bbb0a1f6aa8b54a
92A091A0287A21FE0AC0EDA6061E2AB6
B3EEABB8EE11C2BE770B684D95219ECB
38A79F68E39FFEA775F2DF9988F4F8F7
470fa2b4ae81cd56ecbcda9735803434cec591fa
7769B48695846CACD51EDC1EB55817EA

Google Play 应用市场信息

标题: Cleaner for WhatsApp

评分: 4.5663104 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.lookandfeel.cleanerforwhatsapp

开发者信息: LookAndFeel Lab, 6324583830747629651, None, https://lookfeel.me, contact@lookfeel.me,

发布日期: 2017年9月4日 **隐私政策:** Privacy link

关于此应用:

这个应用程序是一个强大的工具，用于清理通过 WhatsApp 接收和发送的媒体。 WhatsApp 应用程序 Cleaner 最重要的功能： 是您可以定期或按存储限制自动清除 Android 手机或平板电脑上的 WhatsApp 媒体。 WhatsApp Cleaner 为您提供高质量的设计和用户友好的界面。 使用 Cleaner for Whatsapp 将帮助您通过清理 Whatsapp 媒体文件来节省空间。 Cleaner for Whatsapp 应用程序的主要功能： ★ 所有WhatsApp 媒体都在同一个地方。 ★ 轻松点击即可删除指定的 WhatsApp 媒体文件 或所有媒体文件。 ★ 快速删除清理WhatsApp 媒体文件。 ★ 状态保护程序和清洁器。 ★ 启用/禁用自动清理选项以定期或按存储限制清理媒体文件。 ★ 清理前预览所有 WhatsApp 媒体文件类型。 ★ 将重要的媒体文件从 WhatsApp 目录移动到您的设备。 ★ 重复文件查找器：将所有重复文件集中在一个地方，这样您就可以通过删除重复文件轻松恢复手机空间。 ★ 轻松排序文件：在同一窗口中按日期和大小对文件进行排序。 ★ 分别预览发送和接收的媒体。 ★ 高质量的设计和友好的用户界面。 ★ 通知配置选项。 ★ 多国语言。 下载 WhatsApp cleaner 以享受使用 Whatsapp 的乐趣，而不会影响您设备的存储。 WhatsApp Cleaner 专为您打造，如果您喜欢，请随时与您的朋友分享，我们很乐意听取您的反馈。 * 此应用程序不属于 WhatsApp Inc，与其没有任何关系。 ** 感谢 https://icons8.com 提供的图标。

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。