



## ANDROID 静态分析报告



Weicon v2.1.4

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

分析日期: 2025-08-28 10:41:34

## i应用概览

文件名称:	Weicon v2.1.4.apk
文件大小:	32.18MB
应用名称:	Weicon
软件包名:	de.weicon.app
主活动:	de.weicon.app.core.MainActivity
版本号:	2.1.4
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:	61/100 (低风险)
跟踪器检测:	2/432
杀软检测:	经检测, 该文件安全
MD5:	654eeb4f97d3a020cb0bf10579a7cfd1
SHA1:	ea9c96a337bc698ea17ee1004e8efccfc55577fe
SHA256:	2994544f8626244c5d8204cc9acd1f0c1bb1bc03c0cd4bef6e08d5cb2da92d721

## 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
0	10	3	2	0

## 四大组件导出状态统计

Activity组件: 3个, 其中export的有: 0个
Service组件: 10个, 其中export的有: 1个
Receiver组件: 11个, 其中export的有: 2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: True

v2 签名: True

v3 签名: True

v4 签名: False

主题: C=de, ST=NRW, O=nionex

签名算法: rsassa\_pkcs1v15

有效期自: 2014-11-12 10:00:23+00:00

有效期至: 2049-11-03 10:00:23+00:00

发行人: C=de, ST=NRW, O=nionex

序列号: 0x6cd1c327

哈希算法: sha256

证书MD5: e2cb218a161614aa00cf41471f8a23cf

证书SHA1: 3eb3bca965cf12f9fb4a1b5b9ec3669696a9b4a9

证书SHA256: 2d65208a552649a1d6e5cbf81eda1d5bb55d262349ffc7f866f4797f3bb088cb

证书SHA512:

509e8ce427001c5960e9ca55aaf663ac2650f9b8b050423825494d6b9505b445fe4dc52d57a585ee1e45b50f3ddddd7e0e7b25733df9f791bf1907264731400ae

公钥算法: rsa

密钥长度: 2048

指纹: 577ff34efba6c4111f5bc506ed4b6c7747bf9ae6ad91c958133e7ad6e1af6f58

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.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.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.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.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。
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_AD_SERVICES_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_AD_SERVICES_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_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。



2	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。
3	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: 0 | 警告: 5 | 信息: 2 | 安全: 1 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	<a href="#">应用程序记录日志信息,不得记录敏感信息</a>	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MST G-STORAGE-3	<a href="#">升级会员: 解锁高级权限</a>
2	<a href="#">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</a>	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MST G-STORAGE-2	<a href="#">升级会员: 解锁高级权限</a>
3	<a href="#">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</a>	信息	OWASP MASVS: MST G-STORAGE-10	<a href="#">升级会员: 解锁高级权限</a>
4	<a href="#">MD5接口存在哈希冲突的弱哈希</a>	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: MST G-CRYPTO-4	<a href="#">升级会员: 解锁高级权限</a>
5	<a href="#">文件可能包含硬编码的敏感信息,如用户名、密码、密钥等</a>	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MST G-STORAGE-14	<a href="#">升级会员: 解锁高级权限</a>

6	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	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
7	<a href="#">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</a>	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员: 解锁高级权限
8	<a href="#">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</a>	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

## 应用行为分析

编号	行为	标签	文件
00036	从 res/raw 目录获取资源文件	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
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
00202	打电话	控制	升级会员: 解锁高级权限
00203	将电话号码放入意图中	控制	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
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
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
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
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
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
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
00183	获取当前相机参数并更改设置	相机	升级会员: 解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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	3/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.CAMERA
其它常用权限	8/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.ACCESS_WIFI_STATE 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
journeyapps.com	安全	否	IP地址: 216.137.39.33 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: <a href="#">Google 地图</a>
weicon-app.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: <a href="#">Google 地图</a>
www.weicon.de	安全	否	IP地址: 217.5.230.100 国家: 德国 地区: 汉堡 城市: 汉堡 纬度: 53.575253 经度: 10.014778 查看: <a href="#">Google 地图</a>

webdata.weicon.de	安全	否	<p>IP地址: 217.5.230.100                      国家: 德国                      地区: 拜仁                      城市: 纽伦堡                      纬度: 49.447781                      经度: 11.068330                      查看: <a href="#">Google 地图</a></p>
json-schema.org	安全	否	<p>IP地址: 104.26.2.209                      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: <a href="#">Google 地图</a></p>
google.com	安全	否	<p>IP地址: 172.217.12.142                      国家: 美国                      地区: 纽约                      城市: 纽约市                      纬度: 40.713192                      经度: -74.006069                      查看: <a href="#">Google 地图</a></p>
weicon.de	安全	否	<p>IP地址: 185.60.121.212                      国家: 德国                      地区: 汉堡                      城市: 汉堡                      纬度: 53.575253                      经度: 10.014778                      查看: <a href="#">Google 地图</a></p>

## 🌐 URL 链接安全分析

URL信息	源码文件
<ul style="list-style-type: none"> <li>• <a href="http://json-schema.org/draft-04/schema">http://json-schema.org/draft-04/schema</a></li> <li>• <a href="http://json-schema.org/draft-07/schema">http://json-schema.org/draft-07/schema</a></li> <li>• <a href="https://json-schema.org/draft-04/schema">https://json-schema.org/draft-04/schema</a></li> <li>• <a href="http://json-schema.org/draft-06/schema">http://json-schema.org/draft-06/schema</a></li> <li>• <a href="https://json-schema.org/draft-07/schema">https://json-schema.org/draft-07/schema</a></li> <li>• <a href="https://json-schema.org/draft-06/schema">https://json-schema.org/draft-06/schema</a></li> </ul>	org/everit/json/schema/loader/SpecificationVersion.java
<ul style="list-style-type: none"> <li>• <a href="https://webdata.weicon.de/pictures/appbuilder/fallback-news.jpg">https://webdata.weicon.de/pictures/appbuilder/fallback-news.jpg</a></li> <li>• <a href="https://weicon.de/en/company/press/press-releases/">https://weicon.de/en/company/press/press-releases/</a></li> <li>• <a href="https://weicon.de/unternehmen/pressbereich/presse-meldungen/">https://weicon.de/unternehmen/pressbereich/presse-meldungen/</a></li> </ul>	de/weicon/app/components/news/news_detail/NewsDetailItemAdapter.java
<ul style="list-style-type: none"> <li>• <a href="https://google.com">https://google.com</a></li> </ul>	com/tonyodev/fetch2core/FetchCoreUtils.java
<ul style="list-style-type: none"> <li>• <a href="https://webdata.weicon.de/">https://webdata.weicon.de/</a></li> <li>• <a href="https://weicon.de/">https://weicon.de/</a></li> </ul>	de/weicon/app/core/koin/modules/NetworkingModuleKt.java
<ul style="list-style-type: none"> <li>• <a href="https://www.weicon.de/search?ssearch=">https://www.weicon.de/search?ssearch=</a></li> </ul>	de/weicon/app/components/products/screens/detail/ProductDetailViewModeI.java

<ul style="list-style-type: none"> <li>• <a href="https://www.weicon.de/search?search=">https://www.weicon.de/search?search=</a></li> <li>• <a href="https://webdata.weicon.de/">https://webdata.weicon.de/</a></li> <li>• <a href="https://www.weicon.de/unternehmen/pressebereich/pressemeldungen/">https://www.weicon.de/unternehmen/pressebereich/pressemeldungen/</a></li> <li>• <a href="https://www.weicon.de/unternehmen/ueber-uns/ueber-weicon/">https://www.weicon.de/unternehmen/ueber-uns/ueber-weicon/</a></li> <li>• <a href="https://www.weicon.de/unternehmen/messen/">https://www.weicon.de/unternehmen/messen/</a></li> <li>• <a href="https://github.com/journeyapps/zxing-android-embedded">https://github.com/journeyapps/zxing-android-embedded</a></li> <li>• <a href="https://www.weicon.de/karriere-home">https://www.weicon.de/karriere-home</a></li> <li>• <a href="https://journeyapps.com/">https://journeyapps.com/</a></li> <li>• <a href="https://www.weicon.de/unternehmen/ueber-uns/historie/">https://www.weicon.de/unternehmen/ueber-uns/historie/</a></li> <li>• <a href="https://weicon-app.firebaseio.com">https://weicon-app.firebaseio.com</a></li> <li>• <a href="https://www.weicon.de/service">https://www.weicon.de/service</a></li> <li>• <a href="https://weicon.de/">https://weicon.de/</a></li> </ul>	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 <a href="https://weicon-app.firebaseio.com">https://weicon-app.firebaseio.com</a> 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 ( <a href="https://firebaseremoteconfig.googleapis.com/v1/projects/157010766346/namespace/firebase:fetch?key=AlzaSyDFUNU9OguIYmpQh8IGqob-SWQ1AfOc8yc">https://firebaseremoteconfig.googleapis.com/v1/projects/157010766346/namespace/firebase:fetch?key=AlzaSyDFUNU9OguIYmpQh8IGqob-SWQ1AfOc8yc</a> ) 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	<a href="#">Google</a>	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。
ZXing Android Embedded	<a href="#">JourneyApps</a>	Barcode scanning library for Android, using ZXing for decoding.
File Provider	<a href="#">Android</a>	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	<a href="#">Google</a>	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	<a href="#">Google</a>	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	<a href="#">Google</a>	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	<a href="#">Google</a>	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	<a href="#">Google</a>	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	<a href="#">Google</a>	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	<a href="#">Google</a>	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 CrashLytics	Crash reporting	<a href="https://reports.exodus-privacy.eu.org/trackers/27">https://reports.exodus-privacy.eu.org/trackers/27</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>

### 🔑 敏感凭证泄露检测

可能的密钥
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "@7F1200EE"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://weicon-app.firebaseio.com"
"google_api_key" : "AIzaSyDFUNU9OguIYMpOn816nCb-SWQ1AfOc8yc"
"google_app_id" : "1:157010766346:android:1:8573d322ea7bc8924df3"
"google_crash_reporting_api_key" : "AIzaSyDFUNU9OguIYMpOn816nCb-SWQ1AfOc8yc"
"google_maps_api_key" : "AIzaSyCjKgoIavGCzCHc6RstczRdnrFpNgwKQjM"
"library_xingandroidembedded_author" : "JourneyApps"
"library_xingandroidembedded_author_website" : "https://journeyapps.com/"
4988315b7b049d9ae8f5865165b95eb
78557adb0b8a4d489704f67f2911e05e
b275cb6bf837639453786d209711db3
946eca6b182e736e1e90cf82e483715bf
83a027d509ae493faea492f2932c9b77
158cf1945fbad06835117ab1bab2d6ae

460643a974555d792b8f5a6e1a5d323c

## ▶ Google Play 应用市场信息

标题: WEICON

评分: 4.5172415 安装: 5,000+ 价格: 0 Android版本支持: 分类: 办公 **Play Store URL:** [de.weicon.app](https://play.google.com/store/apps/details?id=de.weicon.app)

开发者信息: Weicon GmbH & Co. KG, Weicon+GmbH+%26+Co.+KG, None, <http://www.weicon.com/app>, [app@weicon.de](mailto:app@weicon.de),

发布日期: 2015年11月26日 隐私政策: [Privacy link](#)

关于此应用:

概要 有了这个免费的应用程序,你拥有所有WEICON产品,文档,视频和新闻在眼前。随着各种搜索和扫描功能的帮助下,可以将信息迅速地找到并直接使用。产品展示 查找所有WEICON产品的描述和信息。浏览不同的产品群,并找到产品信息,文档,应用实例或影片在任何时间,使用码扫描器,或搜索功能。直接通过电子邮件发送该信息;快速增加的产品和文档在您的个人收藏夹,或直接从你的问题的应用程序与我们联系。胶粘剂搜索 找到合适的粘结剂 WEICON为您的应用,方便快捷。简单地选择具有几个选项,如材料和温度范围的帮助周围的条件。该WEICON应用程序将直接为您提供一个选择的兼容 WEICON粘合剂。应用领域 找到合适的WEICON产品为您的个人应用领域。从农业技术工具和模具制造行业,该WEICON应用程序为您提供了一个单独的产品选择,针对众多不同行业的特殊需求。应用 基于您的应用提供合适的产品。从一般的应用到应用的专业导航并接受来自WEICON应用了独特的产品推荐。下载 查找的PDF文件(技术数据表(TDS)材料安全数据表(MSDS),画册,宣传册和传单)和视频的快速和简单的列表或使用搜索功能的文档。请求的用户指南或联系WEICON图像数据库。展览 WEICON表示,在许多国家和国际贸易展览和展会。从App自动添加展会到你的日历。让个人的预约在我们的展台与我们的员工之一,直接。新闻 总能从WEICON的最新消息。您将立即通知有关的每一件产品的新颖性或新发展的公司。公司 阅读关于WEICON和浏览历史和 innovation。查找联系方式,为WEICON分支下的位置在互动地图上,或者通过直接印记通过电子邮件推荐WEICON应用程序。代码扫描仪 扫描您的平板电脑或智能手机标签的EAN码,并立即看到所有相关信息,技术数据表及材料安全数据表。由于只是一个水龙头,将数据通过电子邮件发送,存储在您的收藏夹文件或WEICON直接接触。您浏览到视频或进一步的内容秒内使用键盘可言,从我们的宣传册或广告扫描QR码。我的最爱 创建您可以在任何时间,从WEICON应用程序的任何区域访问个人收藏夹文件。装满产品,PDF文档,应用实例和视频文件,并通过电子邮件发送整个文件夹。

## 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