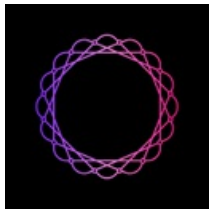
南明离火
移动应用检测平台

ANDROID 静态分析报告



CAARD • v1.1.19

分析日期: 2025-08-01 06:02:34

应用概览

文件名称:	19042f994d0895160463d56f9e313850eaa918dc223d678fbe0d54186c837ac7 v1.1.19.apk
文件大小:	36.3MB
应用名称:	CAARD
软件包名:	net.caard.app
主活动:	net.caard.app.MainActivity
版本号:	1.1.19
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	43/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	8ab19e43a225a73981453bf1d0e8d31e
SHA1:	1d966457a55118de4f83f8fa1ea687334f6d8111b
SHA256:	19042f994d0895160463d56f9e313850eaa918dc223d678fbe0d54186c837ac7

分析结果严重性分布

高危	中危	信息	安全	关注
4	16	2	1	0

四大组件导出状态统计

Activity组件：13个，其中export的有： 3个
Service组件：13个，其中export的有： 1个
Receiver组件：7个，其中export的有： 3个
Provider组件：8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: 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: 2025-01-06 11:54:33+00:00
有效期至: 2055-01-06 11:54:33+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xcb8df70c7131ed43c07f74de25b33902567c95c3
哈希算法: sha256
证书MD5: 452cdc5a4bca6610b4432b4e6b12c22c
证书SHA1: 1e903ac2d981c69cfeecd766c8bcb659ac049677
证书SHA256: d925efa081c85ef40c478fce84b199efaa174bed94eb2c762090f4146851cc6b
证书SHA512:
15d573f2d543a98a383996072e0e605fa322fb091b5d38ba12979bfb1d95d49a9f5f562ccf7e7ee48e9af6b3f6237eb67ec7d124e78907a7388e33e99dbbddf6

公钥算法: rsa
密钥长度: 4096
指纹: ea5ee15c74efc96c154a7350730aa34a1770bda19fe0d88df7ba7d9ec113168c
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.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.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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.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）
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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。
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。
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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
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_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_CUSTOM_AUDIENCE	未知	未知权限	来自 android 引用的未知权限。
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。
net.caard.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.android.vending.CHECK_LICENSE	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
net.caard.app.MainActivity	Schemes: https://, Hosts: dev-links.caard.net, links.caard.net, dev.caard.net, www.caard.net, caard.net, caard.page.link, Path Prefixes: /,
com.facebook.CustomTabActivity	Schemes: @7F0F0058://, fbconnect://, Hosts: cct.net.caard.app,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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: **3** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	App 链接 assetlinks.json 文件未找到 [android:name=net.caard.app.MainActivity] [android:host=https://dev-links.caard.net]	高危	App Link 资产验证 URL（https://dev-links.caard.net/.well-known/assetlinks.json）未找到或配置不正确。（状态码：404）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。

3	App 链接 assetlinks.json 文件未找到 [android:name=net.caard.app.MainActivity] [android:host=https://links.caard.net]	高危	App Link 资产验证 URL（https://links.caard.net/.well-known/assetlinks.json）未找到或配置不正确。（状态码：404）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
4	App 链接 assetlinks.json 文件未找到 [android:name=net.caard.app.MainActivity] [android:host=https://caard.net]	高危	App Link 资产验证 URL（https://caard.net/.well-known/assetlinks.json）未找到或配置不正确。（状态码：301）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
5	Activity (com.facebook.CustomTabActivity) 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	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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。
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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。
9	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。

本报告由南明离火移动安全分析平台生成

10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。
11	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: **1** | 警告: **6** | 信息: **2** | 安全: **0** | 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
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	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

5	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
6	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
7	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
8	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
9	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

应用行为分析

编号	行为	标签	文件
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	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
00009	将游标中的数据放入JSON对象	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
00191	获取短信收件箱中的消息	短信	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
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
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
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
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
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	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
00026	方法反射	反射	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
00012	读取数据并放入缓冲流	文件	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
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
00046	方法反射	反射	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	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
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
00188	获取短信地址	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
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
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
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 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	9/30	android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.VIBRATE
其它常用权限	12/46	android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT com.google.android.gms.permission.AD_ID android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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

本报告由南明离火移动安全分析平台生成

facebook.com	安全	否	**IP地址:** 57.144.222.1 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
docs.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
graph.s	安全	否	No Geolocation information available.
graph-video.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://github.com/baseflow/flutter-permission-handler/issues	j2/p.java
• https://.facebook.com • https://facebook.com	j3/m0.java
• https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures	fa/f.java
• https://%s/%s/%s	g7/c.java
• https://accounts.google.com/o/oauth2/revoke?token=	q4/e.java
• https://play.google.com/store/search?q=otpauth&c=apps	o6/d1.java
• https://facebook.com/device?user_code=%1$s&qr=1	t3/m.java
• https://graph-video.%s • https://graph.%s	j3/i0.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://firebaseremoteconfig.googleapis.com/v1/projects/105799680016 1/namespaces/firebase:fetch?key=AIzaSyAkfLaLEz4sf9nodnmOF0OL1psL4OIM_lE ） 已禁用。响应内容如下所示：
		
		{
		"state": "NO_TEMPLATE"
		}

本报告由南明离火移动安全分析平台生成

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Sign-In	Google	提供使用 Google 登录的 API。
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 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。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
this@createcapturedifneeded.type	wd/d.java
this@abstracttypeconstructor.builtins this@abstracttypeconstructor.paramete	je/g.java

第三方追踪器检测

名称	类别	网址
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.geo.API_KEY" : "AIzaSyDXn9_mVzBL1PO7JmVkB_ClNw-OM3357hw"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"facebook_app_id" : "1341825633853699"
"facebook_client_token" : "6bd70269f561b77fd52a041d9366fa84"

"google_api_key" : "AIzaSyAkfLaLEz4sf9nodnmOF0OL1psL4OlM_lE"
"google_app_id" : "1:1057996800161:android:6b1c491e40ee4c478a70e0"
"google_crash_reporting_api_key" : "AIzaSyAkfLaLEz4sf9nodnmOF0OL1psL4OlM_lE"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
cc2751449a350f668590264ed76692694a80308a
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
9b8f518b086098de3d77736f9458a3d2f6f95a37
c56fb7d591ba6704df047fd98f535372fea00211
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

Google Play 应用市场信息

标题: CAARD - Smart Networking Card

评分: 4.15 **安装:** 1,000+ **价格:** 0 **Android版本支持:** 分类: 开公 **Play Store URL:** net.caard.app

开发者信息: Gainback GmbH, Gainback+Gmbh, None, None, dhairya@caard.net,

发布日期: 2025年1月6日 **隐私政策:** Privacy Link

关于此应用:

轻松连接。更智能的网络。强大的见解。 CAARD 通过无缝、智能的方法重新定义网络，以建立有意义的联系。 CAARD 专为专业人士、企业家和创新者而设计，将您的整个数字身份整合到一个统一的 CAARD 中，可随时随地访问。 - 随时随地共享：通过二维码、点击或直接链接轻松共享您的 CAARD。接收者不需要任何应用程序或特殊工具——只需即时、无缝连接。 - 统一数字身份：将您的社交媒体、支付平台、沟通渠道和专业链接整合到一份完善的 CAARD 档案中。只需轻按一下即可分享所有重要对象。 - 智能交换：在观看者访问您的 CAARD 之前捕获其详细信息，创建有意义的双向连接，这些连接可以无缝数字化并直接添加到您的 CAARD 网络中。 - 扫描和捕获联系人：通过扫描纸质名片、数字二维码或活动徽章，轻松将联系人详细信息数字化。这些详细信息被数字化并无缝添加到您的 CAARD 网络中，从而节省时间并最大限度地减少手动输入。 - 高级分析：实时了解个人资料视图、二维码扫描、参与率等！利用可操作的数据做出明智的决策并优化您的网络策略。 - 隐私和控制：仅在您需要时分享您想要的内容。启用或禁用链接、编辑内容并实时管理您的 CAARD，以实现完全控制和信心十足。 - 工作和个人模式：立即在工作和个人配置文件之间切换以适应您的环境。只需单击一下即可调整您的共享偏好。 - 交互式 CAARD 地图：以前所未有的方式可视化您的网络。通过清晰的交互式地图跟踪您建立联系的地点和时间。 - 个性化注释：为每次交互添加上下文。会议详细信息、共同兴趣、后续提醒——始终触手可及。建立更深入、更有意义的关系。 - 连接套件：下载无缝共享的基本工具：CAARD 个人资料链接的二维码、虚拟背景、用于邮件签名和手机壁纸。在每次互动中最大化您的存在。 - 保存到钱包：将您的 CAARD 添加到手机的数字钱包中，以便随时便捷地访问二维码。还有更多！ 聪明的。直觉的。卡德。 CAARD 不仅仅是一个网络工具，它还是您的简化数字身份。每一次联系都是一次机会，每一次互动都是前进的一步。重新定义世界的连接方式——一次轻按一下。立即下载 CAARD。

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。