南明离火
移动应用检测平台

ANDROID 静态分析报告

Aisle • v12.32

本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-01 12:51:23

应用概览

文件名称:	com.aisle.app v12.32.apk
文件大小:	23.54MB
应用名称:	Aisle
软件包名:	com.aisle.app
主活动:	com.aisle.app.presentation.features.splashScreen.ui.SplashActivity
版本号:	12.32
最小SDK:	26
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:	50/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	6e72a1aa7d1104f9aa9fa23f89c05701
SHA1:	3af6ebd18ffddeb38b2681fc18efeba1bf54bb37
SHA256:	2b62790ae0821b12b5e3e7343a6653ea6f8cdc684f34b74b66f0097ba3d9f66e

分析结果严重性分布

高危	中危	信息	安全	关注
4	19	3	3	1

四大组件导出状态统计

Activity组件：7个，其中export的有： 2个
Service组件：18个，其中export的有： 2个
Receiver组件：16个，其中export的有： 4个
Provider组件：7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: OU=Aisle, CN=Able
签名算法: rsassa_pkcs1v15
有效期自: 2015-04-17 22:57:52+00:00
有效期至: 2040-04-10 22:57:52+00:00
发行人: OU=Aisle, CN=Able
序列号: 0x55318ff0
哈希算法: sha1
证书MD5: aaa0f60245de7f06b8d0b260bbf745bc
证书SHA1: 6a8bec0803006f4eef28836ecd96fe38e2c7c29a
证书SHA256: 3e611e3a0a779518af2cd9468a96ae072d77c9879af19216503e58ea3770503a
证书SHA512:
c26aff573876bc29c01e6f8448b18272ffe95d2b2058ac1d6286832de7472f71df9bd6fd59e4bb81dee04ec6ef852a47257147e6b35dfa[illegible]6b128e8c22c1b9

公钥算法: rsa
密钥长度: 1024
指纹: 25cd7a237dbca573668189e605e932ddde31893c90931808cc3e3318762fd7a6
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.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.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.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.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.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_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.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_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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_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。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量，多用于消息语音功能。
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。
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.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_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。
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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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。
com.aisle.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.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。
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。
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.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。
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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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.aisle.app.presentation.features.splashScreen.ui.SplashActivity	Schemes: https://, aisle://, Hosts: aisle.go.link, www.aisle.co, open, app, aisle.onelink.me, Path Prefixes: /KgP7,
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: **1** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	App 链接 assetlinks.json 文件未找到 [android:name=com.aisle.app.presentation.features.splashScreen.ui.SplashActivity] [android:host=https://aisle.go.link]	高危	App Link 资产验证 URL（https://aisle.go.link/.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。
2	Broadcast Receiver (com.cashfree.pg.core.api.ui.receiver.CFSMSBroadcastReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.phone.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。
3	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。
4	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。
5	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。
6	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。
7	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。

8	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。
9	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: **2** | 警告: **10** | 信息: **2** | 安全: **2** | 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	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
3	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
4	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限

5	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
6	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
7	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
8	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
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
10	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
11	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
12	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

13	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	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
14	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
15	不安全的Web视图实现。可能存在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
16	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
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
00091	从广播中检索数据	信息收集	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
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
00014	将文件读入流并将其放入 JSON 对象	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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00015	将缓冲区（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
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
00191	获取短信收件箱中的消息	短信	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
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
00025	监视要执行的一般操作	反射	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
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
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	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
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
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
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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	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
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
00024	Base64解码后写入文件	反射 文件	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

00080	将录制的音频/视频保存到文件	录制音视频 文件	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00136	停止录音	录制音视频 命令	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
00090	设置录制的音频/视频文件格式	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
00138	设置音频源（MIC）	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
00133	开始录音	录制音视频 命令	升级会员：解锁高级权限
00041	将录制的音频/视频保存到文件	录制音视频	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
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
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
00192	获取短信收件箱中的消息	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.CAMERA android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	13/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH com.google.android.gms.permission.AD_ID android.permission.CHANGE_WIFI_STATE com.google.android.c2dm.permission.RECEIVE 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
sviap.s	安全	否	No Geolocation information available.
payments-test.cashfree.com	安全	否	**IP地址:** 43.204.88.167 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
onelink.to	安全	否	**IP地址:** 178.128.140.200 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.16personalities.com	安全	否	**IP地址:** 172.66.41.42 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
scdn-ssettings.s	安全	否	No Geolocation information available.

cashfreelogo.cashfree.com	安全	否	**IP地址:** 18.238.243.91 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
sattr.s	安全	否	No Geolocation information available.
graph-video.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
facebook.com	安全	否	**IP地址:** 157.144.222.1 **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
notification.aisle.co	安全	否	**IP地址:** 13.227.219.114 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图
sonelink.s	安全	否	No Geolocation information available.
www.aisle.co	安全	否	**IP地址:** 188.114.96.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图
aomedia.org	安全	否	**IP地址:** 185.199.111.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
scdn-stestsettings.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
app.aisle.co	安全	否	**IP地址:** 188.114.97.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图

payments.cashfree.com	安全	否	**IP地址:** 188.114.96.0 国家: 印度 地区: 马哈拉施特拉邦 城市: 孟买 纬度: 19.075975 经度: 72.877380 查看: Google 地图
api.digitap.ai	安全	否	**IP地址:** 188.114.96.0 国家: 印度 地区: 马哈拉施特拉邦 城市: À ôZ {Û5BJAer¼{w o¬ ~Þ JUBèä®Âfr¼p À ôZ {Û5BJA/r¼{w o¬ ~Þ JUBèä®Âjr¼om ´Â öÚ Þ¬!Þ ÖkÀmr¼{w o¬ ~Þ JUBè 纬度: 19.075975 经度: 72.877380 查看: Google 地图
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 13.227.219.114 国家: 荷兰（王国） 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378592 经度: 4.899980 查看: Google 地图
prodsocket.aisle.co	安全	否	**IP地址:** 188.114.96.0 国家: 美国 地区: 印第安纳州 城市: 弗朗西斯科 纬度: 38.333290 经度: -87.447083 查看: Google 地图
apidemo.digitap.work	安全	否	**IP地址:** 188.114.96.0 国家: 印度 地区: 马哈拉施特拉邦 城市: v%v%v%ëv%ìv%Aw%Bw%nw%ow%Ûw%Üw%5x%6x%dx%ex%§x%¨x%õx%öx%Cy%Dy%y% y%éy%ê 纬度: 19.075975 经度: 72.877380 查看: Google 地图
g.co	安全	否	**IP地址:** 142.250.179.142 国家: 荷兰（王国） 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378502 经度: 4.899980 查看: Google 地图

aisle-network.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
receiver.cashfree.com	安全	否	**IP地址:** 188.114.96.0 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
sars.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.
aisleapp.zendesk.com	安全	否	**IP地址:** 216.198.54.6 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
www.cashfree.com	安全	否	**IP地址:** 18.239.36.118 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
api.cashfree.com	安全	否	**IP地址:** 3.108.22.101 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
simpression.s	安全	否	No Geolocation information available.
sandbox.cashfree.com	安全	否	**IP地址:** 3.108.22.101 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
ssdk-services.s	安全	否	No Geolocation information available.

blog.aisle.co	安全	否	**IP地址:** 3.108.22.101 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224338 **经度:** 121.468048 **查看:** 高德地图
apistage.digitap.work	安全	否	**IP地址:** 3.108.22.101 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
smonitorsdk.s	安全	否	No Geolocation information available.
api.digitap.work	安全	否	**IP地址:** 65.2.105.19 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
sinapps.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
default.url	安全	否	No Geolocation information available.
graph.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://%sapp.%s	com/appsflyer/internal/AFj1qSDK.java

本报告由南明离火移动安全分析平台生成

• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1aSDK.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/ReconNetworkRequest.java
• https://%s/%s/%s	F9/c.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	T1/C2086a.java
• https://prodsocket.aisle.co	com/aisle/app/presentation/features/splashScreen/ui/SplashActivity.java
• https://app.aisle.co/v1/	com/aisle/app/data/api/PreSignedApiService.java
• https://default.url	Z0/i.java
• https://sandbox.cashfree.com/pg/ • https://receiver.cashfree.com/pgnextgenconsumer/ • https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/BuildConfig.java
• https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= • https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sonelink.%s/shortlink-sdk/v2 • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id=	com/appsflyer/internal/AFe1ySDK.java
• https://api.digitap.ai/ • https://apistage.digitap.work/ • https://api.digitap.work/ • https://apidemo.digitap.work/	ai/digitap/faceclient/utils/DigiTapEnvironment.java
• https://payments.cashfree.com/ • https://www.cashfree.com/	com/cashfree/pg/core/api/ui/BaseCFWebView.java
• https://sandbox.cashfree.com/pg/ • https://api.cashfree.com/pg/	com/cashfree/pg/core/api/ui/CFWebView.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	T1/C3655a.java
• https://play.google.com/store/apps/details?id=	v4/z0.java
• https://app.aisle.co/v1/ • https://notification.aisle.co/v1/	S2/i.java
• https://facebook.com • https://facebook.com	z5/z.java
• https://graph-video.%s • https://graph.%s	z5/v.java

• https://console.firebase.google.com	o9/b.java
• https://cashfreelogo.cashfree.com/assets_images/pg/wallet/%s%s.png	G5/h.java
• https://cashfreelogo.cashfree.com/assets_images/pg/paylater/%s%s.png	G5/g.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1nSDK.java
• https://cashfreelogo.cashfree.com/assets_images/pg/nb/%s%s.png	G5/b.java
• https://www.16personalities.com/	W2/A1.java
• https://receiver.cashfree.com/pgnextgenconsumer/ • https://sandbox.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/hidden/network/request/OrderStatusNetworkRequest.java
• https://sandbox.cashfree.com/pg/orders/pay/authenticate/ • https://api.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeSubmitOTPRequest.java
• https://sandbox.cashfree.com/pg/orders/pay/authenticate/ • https://api.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeResendOTPRequest.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/FetchSavedCardsNetworkRequest.java
• https://%sadrevenue.%s/api/v2/generic/v6.14.0/android?app_id= • https://%svalidate.%s/api/v • https://%ssdk-services.%s/validate-android-signature • https://%sattr.%s/api/v • https://%slaunches.%s/api/v • https://%sconversions.%s/api/v • https://%sadrevenue.%s/api/v2/log/adimpression/v6.14.0/android?app_id= • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sinapps.%s/api/v • https://aps-webhandler.appsflyer.com/api/trigger	com/appsflyer/internal/AFj1xSDK.java
• https://sandbox.cashfree.com/pg/ • https://receiver.cashfree.com/pgnextgenconsumer/ • https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pgnextgenconsumer/	com/cashfree/pg/core/hidden/utils/URLConstants.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	T8/r.java
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1gSDK.java
• https://receiver.cashfree.com/pgnextgenconsumer/analytics/external/v1/android/ • https://payments.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/ • https://payments-test.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/	I5/C2994a.java

• https://receiver.cashfree.com/pgnextgenconsumer/analytics/external/v1/android/ • https://payments.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/ • https://payments-test.cashfree.com/pgbillpayuiapi/exceptions/sentry/v1/androidparsedatatosentry/	I5/C0847a.java
• https://accounts.google.com/o/oauth2/revoke?token=	O6/f.java
• https://github.com/firebase/firebase-android-sdk • https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure • https://firebase.google.com/docs/database/android/retrieve-data#filtering_data	K8/c.java
• https://console.firebase.google.com/	F8/m.java
• http://g.co/dev/packagevisibility	U0/u.java
• https://blog.aisle.co/	F4/[illegible]2739f.java
• https://notification.aisle.co/v1/	com/aisle/app/data/api/WorkerApiHelper.java
• https://sandbox.cashfree.com/pgnextgenconsumer/order/external/android/config? • https://receiver.cashfree.com/pgnextgenconsumer/order/external/android/config?	com/cashfree/pg/core/hidden/network/request/ConfigNetworkRequest.java
• https://api.cashfree.com/pg/orders/sessions/app • https://sandbox.cashfree.com/pg/orders/sessions/app	com/cashfree/pg/core/hidden/network/request/BaseNetworkRequest.java
• https://blog.aisle.co/	F4/f.java
• https://github.com/lincollincol/amplituda	linc/com/amplituda/exceptions/AmplitudaException.java
• https://api.cashfree.com/pg/ • https://sandbox.cashfree.com/pg/	com/cashfree/pg/core/hidden/network/request/DeleteSavedCardsNetworkRequest.java
• https://www.16personalities.com/	W2/I1.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	A8/f.java
• https://www.aisle.co/privacypolicy.html • https://aisle-network.firebaseio.com • http://onelink.to/aisle • https://www.aisle.co/termsofuse.html • https://aisleapp.zendesk.com/hc/en-us/categories/4458137270417-faq • https://www.instagram.com/aisle.network	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://aisle-network.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/652927018963/namespaces/firebase:fetch?key=AIzaSyADQzw0vh7dmkmxnG8v0Y2A_GnmdS88Eu4 ） 已禁用。响应内容如下所示： 响应码是 403

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 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。
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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
team@aisle.co	com/aisle/app/presentation/features/login/ui/OtpFragment.java
team@aisle.co	自研引擎-S

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
"ACCOUNT_KIT_CLIENT_TOKEN" : "23805a10ac0cd7b5fb86e3f05f4cdf40"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "a6406013aa2b4a62ad7bf48215e7650b"
"facebook_app_id" : "198768123650236"
"facebook_client_token" : "6e70d46a79f7d7e11e05fd3503e92cf4"
"firebase_database_url" : "https://aisle-network.firebaseio.com"
"ga_tracker_key" : "UA-63681596-1"
"google_api_key" : "AIzaSyADQzw1vn7dmkmxnG8v0Y2A_GnmdS88Eu4"
"google_app_id" : "1:652921018363:android:33b9546a4195ac7f"
"google_crash_reporting_api_key" : "AIzaSyADQzw1vn7dmkmxnG8v0Y2A_GnmdS88Eu4"
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
b-c-00ae1fa3-cb15-4776-afcf-ca569d816d12
b-c-06ee692d-fbf6-4d44-83c6-9fdb44943bad
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
9b8f518b086098de3d77736f9458a3d2f6f95a37
c56fb7d591ba6704df047fd98f535372fea00211
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

aXNccyhcZHs2LDh9KXwoXGR7Niw4fSlcc2lzfGlzXHMoXGR7NH0p
470fa2b4ae81cd56ecbcda9735803434cec591fa
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
cc2751449a350f668590264ed76692694a80308a
b-c-55c591d4-8b71-4e06-9dbf-68005f653b51
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
ljEX7eVfoBvBQ3DBnWMj12rapNQygIBA
3E611E3A0A779518AF2CD9468A96AE072D77C9879AF19216503E58EA3770503A
b-c-d6e00d19-8f68-42e6-b4aa-054b56b977e0
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

Google Play 应用市场信息

标题: Aisle — Dating App For Indians

评分: 4.5256114 **安装:** 10,000,000+ **价格:** 0 **Android版本支持:** **分类:** 生活时尚 **Play Store URL:** com.aisle.app

开发者信息: Aisle Network Pvt. Ltd., Aisle+Network+Pvt.+Ltd., None, https://www.aisle.co, team@aisle.co,

发布日期: None **隐私政策:** Privacy link

关于此应用:

Aisle 总部位于班加罗尔，是印度“高意图”约会应用程序的市场领导者。该应用程序由印度人为印度人打造。 Aisle 将来自世界各地的印度或南亚裔人士联系在一起，建立一个相信持久关系的社区。它与据了传统婚恋网站和休闲约会应用程序之间的中间地带。 Aisle 以独特的方式了解印度和南亚的敏感性，使其成为印度（以及海外侨民）增长最快的约会应用程序。它被评为 2020 年印度下载量第二大的约会应用程序。在印度“高意图”约会领域，Aisle 提供的服务是无与伦比的。 特征： 欣赏多样性： Aisle 欣赏印度和南亚文化的细微差别以及定义印度或南亚生活方式的选择。 Aisle 使用的专有算法可确保您根据您的偏好（也许是不可协商的）从母语到信仰找到正确的匹配。女性优先：与 2020 年 HY 相比，Aisle 见证了 2021 年 HY 的女性安装量增加了 40%。根据我们的经验，我们注意到，在高意图约会方面，女性在事情上操纵。因此我们让他们有驱动轮。那么，亲爱的朋友们，你们享受这段旅程怎么样？ 发送“邀请”：“邀请”是最好的对话开始方式，可以在您遇到真正喜欢的个人资料时发送。立即打破坚冰。 安顿下来：过道可以帮助您缩短猜谜游戏的时间，并确保您和您的对手在安顿下来前意见一致。如果您不确定回答这个问题，我们完全理解。 Aisle“礼宾”：这是一项高级应用内服务，您可以在其中获得无限的点赞、无限的邀请、个人资料徽章。如果你正在寻找一场严肃的比赛，过道“礼宾部”是您能拥有的最好的司马阿姨。 排他性：这是Aisle中的一项全新功能，用于衡量与您匹配的排他性。了解他们在过去 3 天内与多少人互动过。 爱情故事：我们深知寻找“真命天子”是一段充满经历的旅程。因此，为了帮助您保持领先地位、正确行事并保持动力，我们整理了一些最感人的故事，讲述我们的用户如何在 Aisle 上遇到特别的人。相信我们，我们非常乐意在博客上介绍您； https://blog.aisle.co/ 应用内购买： 过道邀请 过道加号 过道高级 过道礼宾部 过道提升 通道独家 值得注意的采访： 福布斯： https://bit.ly/3jgf1w6 你的故事： https://bit.ly/3ltl03o

免责声明及风险提示:

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。