南明离火
移动应用检测平台

ANDROID 静态分析报告

aeroLINE CREW

aeroLINE CREW • v5.0.1

分析日期: 2025-08-29 17:11:17

应用概览

文件名称:	aeroLINE CREW v5.0.1.apk
文件大小:	10.89MB
应用名称:	aeroLINE CREW
软件包名:	com.accelaero.aeroLINECREW
主活动:	com.accelaero.aeroLINECREW.MainActivity
版本号:	5.0.1
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	56/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	12baf0d71be043f9ab9bfc2b9ce25fa5
SHA1:	def75616db818e7b6156f60e6944a0a2991a46b9
SHA256:	4e3a26060f4c89c07be8bf3140b998faad9d0b7feea257d58496474a5c8c1f

分析结果严重性分布

高危	中危	信息	安全	关注
2	12	1	3	0

四大组件导出状态统计

Activity组件：4个，其中export的有： 0个
Service组件：13个，其中export的有： 2个
Receiver组件：12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: 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: 2021-06-19 13:38:36+00:00
有效期至: 2051-06-19 13:38:36+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x6b11c536b4b0e00357d2a328cb6172647280227
哈希算法: sha256
证书MD5: 5be57626decbd125b58236fa015c1661
证书SHA1: 7840073bcbba5feae3f06a0c5d63e344b132b2dc
证书SHA256: 1bfe291c3bf3cafc4bad13c627a00bba906cc3cf5732165560fb44fb72e9d3a6
证书SHA512:
313d2c32b6964145c31b79c5e1f523c1e1b886fb83ef99a4c65df602ddf8617d92d94fb65143eb2d2baa858b90df85c92e7a99780813db[illegible]af83236b314ec18

公钥算法: rsa
密钥长度: 4096
指纹: 8c89fe8d4cb000b58798a4a6c90ffebdef9ba00c82d99dfd9314e4fe839351ef
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.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.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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.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.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.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.android.vending.CHECK_LICENSE	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.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.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。

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	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。

2	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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。
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	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。

代码安全漏洞检测

高危: **2** | 警告: **4** | 信息: **1** | 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	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	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	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
5	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
6	MD5是已知存在哈希冲突的哈希	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
7	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
8	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

9	此应用程序具有防止窃听攻击的功能	安全	OWASP MASVS: MSTG-PLATFORM-9	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
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
00028	从assets目录中读取文件	文件	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
00036	从 res/raw 目录获取资源文件	反射	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
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
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
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
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
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
00043	计算WiFi信号强度	信息收集 WiFi	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
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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	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
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	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	5/30	android.permission.CAMERA android.permission.WRITE_CALENDAR android.permission.READ_CALENDAR android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	9/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

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

pinterest.com	安全	否	**IP地址:** 151.101.128.84 **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
twitter.com	安全	否	**IP地址:** 151.101.128.84 **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
• http://help.dottoro.com/lcbixvwm.php • https://bugzilla.mozilla.org/show_bug.cgi?id=947588 • https://fjl.asqs.net/index.php • https://rbg.asqs.net/index.php • https://aviationweather.gov/api/data/dataserver?requestType=retrieve&dataSource=tafs&startTime • https://cesarg92.isaaviations.com/admin/aeroLineCrewAdmin • https://crewg9.isaaviations.com/cesar-web-intranet-portal/webIntranetPortal • https://crewportaler.isa.ae • https://cesarapi.airarabia.com/admin/aeroLineCrewAdmin • http://www.staff.science.uu.nl • https://crewg6.accelaero.com/admin/aeroLineCrewAdmin • https://api.checkwx.com/metar • https://crewe5.accelaero.cloud/admin/aeroLineCrewAdmin • https://github.com/csstree/stylelint-validator/issues/29 • https://crewg9.isaaviations.com • https://cesarad.airarabia.com • https://cesar.airarabia.com/cesar-web-intranet-portal/webIntranetPortal • https://crewportal9p.accelaero.com • https://crewad.accelaero.cloud/admin/aeroLineCrewAdmin • https://cesar9p.isaaviations.com/admin/aeroLineCrewAdmin • https://redux.js.org/Errors?code • https://github.com/csstree/csstree/issues • https://github.com/axios/axios.git • https://crewportal9p.accelaero.com/cesar-web-intranet-portal/webIntranetPortal • https://crewportalg6.accelaero.com/cesar-web-intranet-portal/webIntranetPortal • https://crew3o.accelaero.cloud/admin/aeroLineCrewAdmin • https://cesarreports.airarabia.com • http://invertase.link/android • https://crew9p.isaaviations.com/cesar-web-intranet-portal/webIntranetPortal • https://react-native-community.github.io/async-storage/docs/advanced/jestnnIf • https://axios-http.com • https://cesarreports.accelaero.cloud • https://play.google.com/store/apps/details?id • https://cesaregypt.airarabia.com • https://cesaregypt.airarabia.com/cesar-web-intranet-portal/webIntranetPortal • https://www.sitepoint.com/css3-cursor-styles • https://cesar.airarabia.com	

• http://help.dottoro.com/lclhnthl.php • https://github.com/mdn/data/pull/431 • http://invertase.link/ios • https://crewg6.isaaviations.com • https://aby.asqs.net/index.php • http://help.dottoro.com/lcxquvkf.php • https://crew9p.accelaero.com/admin/aeroLineCrewAdmin • https://github.com/axios/axios/issues • https://cesarreports.isa.ae • https://crewer.isaaviations.com/cesar-web-intranet-portal/webIntranetPortal • https://cesarad.airarabia.com/cesar-web-intranet-portal/webIntranetPortal • https://cesarmaroc.airarabia.com • http://fb.me/use-check-prop-types • http://phrogz.net/tmp/canvas_image_zoom.html • https://cesarmaroc.airarabia.com/cesar-web-intranet-portal/webIntranetPortal • http://cssdot.ru/%D0%A1%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D1%87%D0%BD%D0%B8%D0%BA_CSS/color-i305.html • https://github.com/lahmatiy • https://docs.swmansion.com/react-native-gesture-handler/docs • https://crewportaler.isa.ae/cesar-web-intranet-portal/webIntranetPortal • https://cesarg6.isaaviations.com/admin/aeroLineCrewAdmin • https://aviationweather.gov/api/data/dataserver?requestType=retrieve&dataSource=metars&startTime • https://crewreports.isaaviations.com • https://crewg94.isaaviations.com/admin/aeroLineCrewAdmin • http://css-infos.net/property/-webkit-appearance • https://drafts.fxtf.org/css-masking-1 • http://help.dottoro.com/lcrthhhv.php • https://drive.google.com/open?id=1MBHJXeRxMLLwHFpqbgTdEPsFAnMM0cz7 • https://github.com/szimek/signature_padn • http://www.ummulqura.org.sa/index.aspx • http://help.dottoro.com/lcbkewgt.php • https://mac.asqs.net/index.php • https://clients3.google.com/generate_204 • https://crewer.isaaviations.com • https://itunes.apple.com • https://crewreports.accelaero.com • https://crewportalg6.accelaero.com • http://momentjs.com/guides • https://crewg6.isaaviations.com/cesar-web-intranet-portal/webIntranetPortal • https://crew9p.isaaviations.com	自研引擎-A
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramStoriesShare.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.java

• https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.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/772560439909/namespaces/firebase:fetch?key=AIzaSyANdVJuZhgIp0J6d911ZhSyTmFGck2Lbhk ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

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 必须集中的最新信息。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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 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
"google_api_key" : "AIzaSyANdVJuZhgIp0J6d911ZhSyTmFGck2LbhU"
"google_app_id" : "1:772560439909:android:9b5e99a5143c48911c948c"
"google_crash_reporting_api_key" : "AIzaSyANdVJuZhgIp0J6d911ZhSyTmFGck2LbhU"

Google Play 应用市场信息

标题: aeroLINE CREW

评分: 2.8952382 **安装:** 5,000+ **价格:** 0 **Android版本支持:** **分类:** 效率 **Play Store URL:** com.accelaero.aeroLINECREW

开发者信息: ISA (Information Systems Associates), ISA+(Information+Systems+Associates), None, https://accelaero.com, ddey@accelaero.com,

发布日期: 2021年7月4日 **隐私政策:** Privacy link

关于此应用:

aeroLINE-CREW 移动应用程序 Accelaero 最新的船员应用程序。 借助 aeroLINE-CREW，航空公司机组人员可以随时随地通过手持设备实时访问与其航班相关的信息、名册提交报告以及管理与运营航班相关的许多必需任务。我们正在不断增强应用程序的更多功能和特性，敬请期待未来的更新。 请使用 aeroLINE CREW 门户凭据登录应用程序。 关于 Accelaero 自 2005 年以来，信息系统协会 (ISA) 是信息技术领域的佼佼者，为全球旅行和航空业提供一流的技术解决方案。我们提供广泛的量身定制的航空技术解决方案，满足各个方面的需求组织的。技术支援： 如果您在 Accelaero 客户航空公司工作并对应用程序有任何疑问或建议，请通过 mobile.dev@accelaero.com 与我们联系 aeroLINE Crew App 是 Information Systems Associate (AccelAero) 的版权

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。