南明离火
移动应用检测平台

ANDROID 静态分析报告

gocrew : v27.3

分析日期: 2025-07-05 06:47:07

应用概览

文件名称:	gocrew v27.3.apk
文件大小:	9.63MB
应用名称:	gocrew
软件包名:	com.dexit.gocrew
主活动:	com.example.gocrew.login.LoginActivity
版本号:	27.3
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:	60/100 (低风险)
跟踪器检测:	2/432
杀软检测:	AI评估：安全
MD5:	77f2d09f2d531897bf609718ed5f30fa
SHA1:	3cb5425da4c0cd7c8905cd9db4c08e93f727749f
SHA256:	208e9deaef09df12b039f04c43726cf98228744a2597c444afd306ef2b5fc178

分析结果严重性分布

高危	中危	信息	安全	关注
0	11	3	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 1个
Service组件：10个，其中export的有： 2个
Receiver组件：5个，其中export的有： 3个

Provider组件：4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: 2023-05-22 11:36:23+00:00
有效期至: 2053-05-22 11:36:23+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x6822af42910e28915f260beec9f6655d3a45c382
哈希算法: sha256
证书MD5: deade1c81900f39387c0ca024daf8ac8
证书SHA1: 0dfa82811060f021f576e3620c7f5a63389646c5
证书SHA256: 6a2c6ec123647bbbc28e5da6f56815911748b0f483339d5a6cdce8b127e79e9b
证书SHA512:
99af041d7a2a4ed914b3bda86cf273f6e9b62c46e8a798c04db879ffda8fa438d7811f8ff14a9509ce0c62c560797d6fb58051a6f8d76dfc05b0d2f9f76760bc

公钥算法: rsa
密钥长度: 4096
指纹: c0296ccad455d5ecf80061fd8dbb2fc60b8eb0ebc6c52dc70239cfa460e47238
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.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.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.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.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.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。

android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.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.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.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.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.dexit.gocrew.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: **8** | 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、MediaPlayer 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	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。
3	Activity (com.example.gocrew.supervisor.checkinemployment.EmployeeImage) 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	Broadcast Receiver (com.example.gocrew.servicebg.BroadCasting) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
5	Service (com.example.gocrew.others.MyFirebaseMessagingService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
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 (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。
8	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: **1** | 信息: **2** | 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	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	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
4	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

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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 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
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

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.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.VIBRATE android.permission.WAKE_LOCK

其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY android.permission.ACCESS_BACKGROUND_LOCATION android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 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
app.dexgo.co	安全	否	**IP地址:** 204.197.244.110 **国家:** 美国 **地区:** 伍治亚州 **城市:** 亚特兰大 **纬度:** 33.748795 **经度:** -84.387543 **查看:** Google 地图
porter-system.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:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://app.dexgo.co:3333/api/ • https://app.dexgo.co/api/v1/public/index.php/ • https://app.dexgo.co:3000/api/	com/example/gocrew/others/WebUrls.java
• https://play.google.com/store/apps/details?id=com.dexit.gocrew	com/example/gocrew/login/LoginActivity.java
• https://porter-system.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://porter-system.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/178279551801/namespaces/firebase:fetch?key=AIzaSyC3Kseo0RHXMbAVxdNE-_IJzWV6sPpe8Dc ） 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。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://porter-system.firebaseio.com"
"google_api_key" : "AIzaSyC3Kseo0RHXMbAVxdNE-_lJzWV6sPpe8Dc"
"google_app_id" : "1:178279551801:android:85b4faf54e3efb64798ee8"
"google_crash_reporting_api_key" : "AIzaSyC3Kseo0RHXMbAVxdNE-_lJzWV6sPpe8Dc"
"password" : "Password"
afc0d1203d23bb10484b7a42a2ac8bba
933057815691b4991aedf5fe8e36e2a1
57a030dc35ad63452e242e7aeb42859c
71485509f156acc397b4d3b45321b554

Google Play 应用市场信息

标题: gocrew - smart workforce

评分: 3.8 **安装:** 500+ **价格:** 0 **Android版本支持:** **分类:** 效率 **Play Store URL:** com.dexit.gocrew

开发者信息: Dexgo Inc., 8840130371298396190, None, https://www.dexgo.co, support@dexgo.co,

发布日期: 2023年5月23日 **隐私政策:** Privacy Link

关于此应用:

高效智能的劳动力管理解决方案 有效的设施管理在很大程度上依赖于管理和维护场所的劳动力。提高员工的生产力有助于产生更好的结果并节省不必要的管理费用。 gocrew 旨在帮助您管理、监控和优化您的劳动力以获得更好的结果。 任务管理 针对重复任务和临时任务的内置任务管理，通过实时监控每项任务的进度，帮助您更有效地管理日常工作。了解哪些任务按时完成、哪些任务延迟、谁的工作效率更高以及您的员工的利用率等等。 监控效用和效率 监控员工的效率和效用，并确定高效运营所需的最佳数量。减少不必要的管理成本并带来运营利润。 员工室内追踪 跟踪员工值班时的室内活动，监控他们在不同地点花费的时间，并了解在生产性地点花费了多少时间。 实现运营效率 通过优化运营、高效利用劳动力以及节省成本，提高您的设施运营效率。

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。