南明离火
移动应用检测平台

ANDROID 静态分析报告

fieldd • v4.2.4

分析日期: 2025-08-04 09:33:32

应用概览

文件名称:	fieldd v4.2.4.apk
文件大小:	12.33MB
应用名称:	fieldd
软件包名:	com.refreshbookings.staff
主活动:	com.refreshbookings.staff.MainActivity
版本号:	4.2.4
最小SDK:	27
目标SDK:	34
加固信息:	未加壳
开发框架:	Cordova
应用程序安全分数:	56/100 (中风险)
跟踪器检测:	4/432
杀软检测:	经检测，该文件安全
MD5:	7fed74a449eee527eb43a41e5a7cb472
SHA1:	7fc07f0b2cad1402[illegible]e25034df7dc2897d16ff32
SHA256:	518514031b7[illegible]0335915965ab4b916418[illegible]9b9ef1a90ab29be5a937353279f982

分析结果严重性分布

高危	中危	信息	安全	关注
0	20	3	2	0

四大组件导出状态统计

Activity组件：4个，其中export的有： 4个
Service组件：12个，其中export的有： 2个
Receiver组件：6个，其中export的有： 3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: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-26 04:54:17+00:00
有效期至: 2049-08-26 04:54:17+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xa3380241f4a23ffdfb93634867464324d4235645
哈希算法: sha256
证书MD5: f395d76cbd79548dfad04558ce2369d6
证书SHA1: 3ea1af96d2367347e4d9142c4dc070ee7277eeab
证书SHA256: 0f23b9d3d7561c9047604f2c6f84b134700d5202e5e222465adc7e5f3d10c395
证书SHA512:
6a3b071a082f763322c895c3c79f20d6f8f2904613e1f967d3efb81416c0892954a4536e2d73dbad3af52f3be8e4e33dac177e4043dd9150fd4d0f7074fe12b7

公钥算法: rsa
密钥长度: 4096
指纹: b41384d732e87a78a931822163737ede902c807ac3e9962a1bb2442a92fd67[illegible]
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.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.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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_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_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_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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。

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.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。
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
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。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
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。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
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.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
android.hardware.location	未知	未知权限	来自 android 引用的未知权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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。

本报告由南明离火移动安全分析平台生成

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。
com.refreshbookings.staff.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.refreshbookings.staff://,

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: **0** | 警告: **11** | 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。
3	Activity (org.apache.cordova.firebase.OnNotificationReceiverActivity) 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 (nl.xservices.plugins.ShareChooserPendingIntent) 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.marianhello.bgloc.sync.SyncService) 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.marianhello.bgloc.BootCompletedReceiver) 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。
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	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。
9	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。
10	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。

11	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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。

代码安全漏洞检测

高危: **0** | 警告: **7** | 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	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
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	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	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
7	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限

8	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
9	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
10	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00039	启动网络服务器	控制 网络	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
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
00036	从 res/raw 目录获取资源文件	反射	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
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	短信 通话记录 信息收集	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
00012	读取数据并放入缓冲流	文件	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
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

00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	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
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
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
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
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
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
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00195	设置录制文件的输出路径	录制音视频 文件	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
00007	Use absolute path of directory for the output media file path	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
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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO
其它常用权限	13/46	android.permission.INTERNET android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_IMAGES android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_NETWORK_STATE android.permission.AUTHENTICATE_ACCOUNTS com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT 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
api.whatsapp.com	安全	否	**IP地址:** 57.144.223.32 **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
logback.qos.ch	安全	否	**IP地址:** 195.15.222.169 **国家:** 瑞士 **地区:** 日内瓦 **城市:** 兰西 **纬度:** 46.189812 **经度:** 6.114410 **查看:** Google 地图

refresh-158805.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
share.here.com	安全	否	**IP地址:** 18.239.50.37 **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
mindprod.com	安全	否	**IP地址:** 65.110.21.43 **国家:** 加拿大 **地区:** 不列颠哥伦比亚省 **城市:** 温哥华 **纬度:** 49.281139 **经度:** -123.12[illegible] **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/pvorb/node-md5 • https://js.qa.finix.com/v/1/finix.js • https://github.com/videojs/video.js/issues/2617 • http://jsperf.com/b64tests • https://momentjs.com/timezone/docs • https://fieldd-images.s3.ap-southeast-2.amazonaws.com • https://github.com/ionic-team/cordova-plugin-ionic-webview • https://chat.stenciljs.com • https://angular.io/license • https://fieldd.firstpromoter.com • https://fieldd.co/privacy • https://validator.ianaic.com • https://markerjs.com • https://pp.payfabric.com/payment • https://github.com/dpa99c/cordova-plugin-firebasex • https://localforage.github.io/localForage • https://ng.co/ng/security • https://dnuxhy2xsjuze.cloudfront.net • https://fieldd.co/terms • https://github.com/xmartlabs/cordova-plugin-market • https://apis.google.com/js/api.js • https://sandbox.payfabric.com/payment • http://github.com/dpa99c • https://git.io/vMpjB • https://sandbox.web.squarecdn.com/v1/square.js • https://web.squarecdn.com/v1/square.js • https://github.com/dpa99c/phonegap-launch-navigator • https://github.com/phonegap/phonegap-plugin-barcodescanner • https://github.com/ionic-team/stencil/issues/5457	

- http://github.com/MaximBelov/cordova-plugin-chooser.git
- http://ionic.io
- https://docs.sentry.io/platforms/javascript/best-practices/browser-extensions
- https://fieldd.me/welcome_video_0824_mp4
- https://github.com/cordova-plugin-camera-preview/cordova-plugin-camera-preview
- https://github.com/mauron85/cordova-plugin-background-geolocation
- https://www.google.com/recaptcha/api.js
- https://github.com/pwlin/cordova-plugin-file-opener2
- https://js.stripe.com/v3
- https://www.payfabric.com/payment
- http://www.iana.org/assignments/character-sets
- http://momentjs.com/timezone/docs
- https://fieldd-images.s3-ap-southeast-2.amazonaws.com
- https://github.com/lodash/lodash
- https://www.iaptic.com
- https://refresh-158805.firebaseio.com
- https://stenciljs.com/docs/properties
- https://ngrx.io/guide/store/configuration/runtime-checks
- https://vjs.zencdn.net/vttjs/0.14.1/vtt.min.js
- https://github.com/whiteoctober/cordova-plugin-app-version
- https://infotracer.com/img/plates/blank
- https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE
- https://docs.sentry.io/platforms/javascript/guides/angular
- http://brianleroux.github.com/lawnchair
- https://admin.fieldd.co
- https://api.fieldd.co
- https://fieldd.me/appDemo
- https://www.google.com/recaptcha/enterprise.js?render=6LfIZVMpAAAAAGhn8PP3bv9khQn9v9S079CwwG_
- https://github.com/NeoLSN/cordova-plugin-android-permissions
- https://github.com/cartant/rxjs-etc
- https://a.com
- https://github.com/jindw/xmldom/graphs/contributors
- https://qa.payfabric.com/payment
- http://creativecommons.org/publicdomain/zero/1.0
- https://fieldd.me/welcome_video_0824
- https://help.fieldd.co/en/articles/5168079-i-want-to-use-square-for-payments
- https://datatracker.ietf.org/doc/html/draft-pantos-hls-rfc8216bis-19
- https://fieldd.me/welcome_video_0824_poster
- https://github.com/MaximBelov/cordova-plugin-chooser
- http://momentjs.com/guides
- https://github.com/christocracy/cordova-plugin-background-geolocation
- https://dev-us2.payfabric.com/payment
- https://github.com/lbynum/cordova-plugin-building
- http://zxing.appspot.com/generator
- https://api.openweathermap.org/data/2.5/weather
- http://radio.uxder.com
- https://mpp.qualpay.com/hosted/embedded/js/qp-embedded-sdk.min.js
- http://crity.com
- https://fieldd-images.s3.ap-southeast-2.amazonaws.com/fieldd_default_images/no-photo-available.png
- https://fieldd-images.s3.amazonaws.com
- http://underscorejs.org
- https://github.com/EddyVerbruggen/SocialSharing-PhoneGap-Plugin/issues/1052
- https://api.fieldd.co:9100
- https://tools.ietf.org/html/draft-pantos-http-live-streaming-23
- https://openjsf.org
- https://github.com/xmldom/xmldom/graphs/contributors
- https://stenciljs.com/docs/custom-elements
- https://github.com/chemerisuk/cordova-plugin-app-review
- https://mozilla.github.io/localForage

白帽引擎-A

• https://admin.fieldd-staging.com • https://www.google.com/recaptcha/enterprise.js?render • https://developer.apple.com/documentation/appstorereceipts/expiration_intent • http://www.workingedge.co.uk • https://stenciljs.com/docs/templating-jsx	
• http://logback.qos.ch/codes.html#smtp_no_layout	ch/qos/logback/core/net/SMTPAppenderBase.java
• http://logback.qos.ch/codes.html#syslog_layout	ch/qos/logback/core/net/SyslogAppenderBase.java
• http://logback.qos.ch/codes.html#tbr_fnp_not_set • http://logback.qos.ch/codes.html	ch/qos/logback/core/CoreConstants.java
• http://logback.qos.ch/codes.html#appender_order	ch/qos/logback/core/joran/action/AppenderRefAction.java
• 8.1.2.2 • 8.1.2.1 • 8.1.2.3	io/grpc/okhttp/OkHttpServerTransport.java
• http://logback.qos.ch/codes.html#receiver_no_port • http://logback.qos.ch/codes.html#receiver_no_host	ch/qos/logback/classic/net/SocketReceiver.java
• http://play.google.com/store/account/subscriptions • http://play.google.com/store/paymentmethods	cc/fovea/PurchasePlugin.java
• http://logback.qos.ch/codes.html#sbtp_size_format	ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java
• http://logback.qos.ch/codes.html#layoutinsteadofencoder	ch/qos/logback/core/OutputStreamAppender.java
• https://share.here.com/r/mylocation • https://share.here.com/r/	uk/co/workingedge/LaunchNavigator.java
• https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
• 127.0.0.1	io/grpc/okhttp/OkHttpClientTransport.java
• http://mindprod.com	com/mindprod/ledatastream/LEDataInputStream.java
• http://logback.qos.ch/css/classic.css	ch/qos/logback/classic/html/UrlCssBuilder.java
• http://logback.qos.ch/codes.html#rfa_no_rp • http://logback.qos.ch/codes.html#rfa_file_after • http://logback.qos.ch/codes.html#rfa_no_tp • http://logback.qos.ch/codes.html#rfa_collision	ch/qos/logback/core/rolling/RollingFileAppender.java
• http://logback.qos.ch/codes.html#tbr_fnp_not_set • http://logback.qos.ch/codes.html#tbr_fnp_prudent_unsupported • http://logback.qos.ch/codes.html#fwrp_parentfilename_not_set	ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java

• http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java
• http://logback.qos.ch/codes.html#socket_no_port • http://logback.qos.ch/codes.html#socket_no_host	ch/qos/logback/core/net/AbstractSocketAppender.java
• http://logback.qos.ch/codes.html#missingrightparenthesis	ch/qos/logback/core/pattern/parser/Parser.java
• http://logback.qos.ch/codes.html#1andonly1	ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java
• http://logback.qos.ch/codes.html#renamingerror	ch/qos/logback/core/rolling/helper/RenameUtil.java
• https://refresh-158805.firebaseio.com	自研引擎-8

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://refresh-158805.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/151087308856/namespaces/firebase:fetch?key=AIzaSyCnPatATdh81ftcM7RUq8nVkiZgmWSNz8 ） 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 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。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

邮箱地址敏感信息提取

EMAIL	源码文件
someone@domain.com	nl/xservices/plugins/SocialSharing.java
support@card.io	io/card/payment/CardScanner.java
support@card.io	io/card/payment/CardIOActivity.java

第三方追踪器检测

名称	类别	网址
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
凭证信息=> "launchmyvgator.GOOGLE_API_KEY" : "AIzaSyDszu3fwVXQdYZsExyZz2_N9sibIzHyO_E"
Google_Drive_API_Key: AIzaSyBcvAPYHf_4w2DnIgc_gceEIHUqsrq6i4E
Google_Drive_API_Key: AIzaSyDszu3fwVXQdYZsExyZz2_N9sibIzHyO_E
"firebase_database_url" : "https://refresh-158805.firebaseio.com"
"google_api_key" : "AIzaSyCnPat3ATdh81ftcM7RUq8nVkiZgmWSNz8"

"google_app_id" : "1:151087308856:android:59972fa3661fe58aad06cd"
"google_crash_reporting_api_key" : "AIzaSyCnPat3ATdh81ftcM7RUq8nVkiZgmWSNz8"
"plugin_bgloc_content_authority" : "com.refreshbookings.staff"

Google Play 应用市场信息

标题: fieldd

评分: 4.627451 **安装:** 5,000+ **价格:** 0 **Android版本支持:** **分类:** 效率 **Play Store URL:** com.refreshbookings.staff

开发者信息: fieldd.co, 8280850732620068322, None, https://www.fieldd.co, hello@fieldd.co,

发布日期: 2019年8月25日 **隐私政策:** Privacy link

关于此应用:

对于想要在一天内安排更多工作并更快获得报酬的家庭和汽车服务公司来说，Fieldd 是排名第一的应用程序。选择很简单。 **我们的应用程序可以免费使用，付费版本中还提供额外的高级功能。** 为什么选择菲尔德？ 让您的工作日充满活力 - 日常任务减少 80%：节省时间并提高生产力。 - 消除文书工作：实现数字化并简化您的工作流程。 - 更快的付款：通过集成的付款选项加快您的现金流。 给您的客户留下深刻印象 - GPS 实时跟踪：让客户了解实时更新。 - 自动短信提醒：自动发送进度更新。 - 品牌传播：提供专业的电子邮件、发票和报价。 掌控您的业务 - 24/7 工作接待：即使在工作时间之外，也不会错过任何工作。 - 自动调度和调度：简化工作分配。 - 内置质量控制：确保每项工作都符合您的标准。 - 团队沟通：使用实时聊天和推送通知保持联系。 更快获得付款 - 集成销售点：无缝接受各种支付方式。 - 在线支付链接：向客户发送安全支付链接。 提供品牌/白标应用程序 - 移动服务应用程序：定制设计并在 30 天内推出。 - 移动客户应用程序：定制设计并在 30 天内发布。 适用于家居和汽车服务的一体化软件 - 移动应用 - 销售点 - POS - CRM 网络仪表板 - 客户门户 - 在线调度 - 移动客户应用程序 - 网上支付 改善您的客户体验并简化员工调度和派遣，以有效地处理更多工作。 旨在与您的业务一起成长 Fieldd 可根据您的业务进行扩展。如果您是全新企业，或者是小范围内的特许经营企业，Fieldd 将随着您的业务一起成长。专注于发展您的业务，而 Fieldd 负责处理物流、给客户留下深刻印象并安排您的日程安排。 fieldd 应用程序非常适合通过预约或像 Uber 这样按需派遣员工的现场服务公司。 使用 fieldd 进行更好的管理和调度的家庭服务公司： 家庭清洁服务 汽车细节 汽车清洁 汽车 暖通空调 锁匠 老年护理 家电维修 美容服务 船舶细节 房屋检查 地毯清洗 承包商 电脑及IT维修 电工 玻璃和挡风玻璃维修 杂工服务 洗衣及干洗 庭院卡和景观美化 按摩治疗师 力学 移动机械 手机维修 音乐课 公证人 换油 画家 私人教练 宠物美容 摄影服务 物理治疗师 水管工 泳池清洁 泳池维护 高压清洗 房地产摄影 划痕和凹痕修复 PDR - 免漆凹痕去除 除雪 拼车和出租车 除害虫 在家兽医 窗户清洁 窗口着色 加入智慧服务公司行列 您是一名需要更好的调度解决方案的工作人员吗？想成为家居服务行业的巨头吗？ Fieldd 的应用程序是为您设计的。 使用 Fieldd 提高您的可用性和效率。准备好改变您的业务了吗？ 了解 Fieldd 如何帮助您安排更多工作并更快获得报酬。立即免费试用 Fieldd，看看有何不同！

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。