南明离火

移动应用检测平台

ANDROID 静态分析报告

TRIPP Mobile • v1.17.0

分析日期: 2025-07-06 09:46:40

应用概览

文件名称:	TRIPP Mobile v1.17.0.apk
文件大小:	19.55MB
应用名称:	TRIPP Mobile
软件包名:	com.tripp.companion
主活动:	com.braze.unity.BrazeUnityPlayerActivity
版本号:	1.17.0
最小SDK:	29
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:	39/100 (高风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	45605620a81d72188951786604 75e996
SHA1:	70a9164ae7411d3e7737e7be7c71375e5720662
SHA256:	a2e387f07f737b4ff25aa880ac2fb7b34faf6e66dbd1e743234577de3b8d1bed

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
5	19	4	0	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 2个
Service组件：17个，其中export的有： 5个
Receiver组件：6个，其中export的有： 1个
Provider组件：5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: False
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: 2018-07-04 00:44:46+00:00
有效期至: 2048-07-04 00:44:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x9dfd92aab837b17355faf732d24ab874cf358c06
哈希算法: sha256
证书MD5: e56c52c82bfed81f1878c7188a00b032
证书SHA1: 765a13b09ea5bef2fd8dcb4d7d1e060de3db9db1
证书SHA256: 354fb00d03703b921f1f7af4c1d10189d4567d98ac79ee3bb08fa52e83a12fb1
证书SHA512:
7cb82e3f8eb13027cb44f717422dfabdd6bdd37ea379f835c6c3917906f30ad103562ff4bec6478c74fe9e0d6c967974b3e006706da66b71d503f315cb8f9701

公钥算法: rsa
密钥长度: 4096
指纹: 20a839d6ddc5aaaf173e453868ad87c945a3f29eb1b626f98b6123e5046b0238
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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。
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.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.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.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.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.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。
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.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_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
com.google.android.providers.gsf.permission.READ_GSERVICES	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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
com.tripp.companion.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.tripp.companion.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.braze.unity.BrazeUnityPlayerActivity	Schemes: tripp://, http://, https://, Hosts: share.tripp.com, cm-redirect.azurewebsites.net,
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: **0** | 警告: **10** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	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。
3	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。

4	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。
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	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。
7	Service (com.cm.mediaplayer.CMPlaybackService) 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。
8	Service (com.kdg.toast.plugin.PedometerService) 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。
9	Service (com.google.android.gms.messaging.cpr.MessageForwardingService) 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。
10	Activity 设置了 TaskAffinity 属性 (com.braze.push.NotificationTrampolineActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。

代码安全漏洞检测

高危: **4** | 警告: **1** | 信息: **3** | 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	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
3	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
4	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
5	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
6	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
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	该文件是World Readable。任何应用程序都可以读取文件	高危	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
9	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
10	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
11	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。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
12	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
13	此应用程序使用SQL Cipher，确保密钥没有硬编码在代码中	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
14	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

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

本报告由南明离火移动安全分析平台生成

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
00091	从广播中检索数据	信息收集	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
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
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
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
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
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
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
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
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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
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

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.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	11/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.google.android.gms.permission.AD_ID android.permission.BLUETOOTH com.google.android.c2dm.permission.RECEIVE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACTIVITY_RECOGNITION android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE

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
smonitorsdk.s	安全	否	No Geolocation information available.
sondheim.braze.com	安全	否	**IP地址:** 172.64.144.252 **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
slaunches.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
mobile.events.data.microsoft.com	安全	否	**IP地址:** 20.189.173.10 **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
sinapps.s	安全	否	No Geolocation information available.
sattr.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.
tripp-prod.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
iamcache.braze	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
sdk.iad-01.braze.com	安全	否	**IP地址:** 172.64.148.188 **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.
sonelink.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 13.226.210.33 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
in.appcenter.ms	安全	否	**IP地址:** 4.153.25.42 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 博伊顿 **纬度:** 36.667641 **经度:** -78.387497 **查看:** Google 地图
sconversions.s	安全	否	No Geolocation information available.
scdn-stes.settings.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
dust.k8s.test-001.d-usw-2.braze.com	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.

www.braze.com	安全	否	**IP地址:** 104.17.228.60 **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

URL 链接安全分析

URL信息	源码文件
• https://cdp.cloud.unity3d.com/v1/events • https://dashboard.unity3d.com • https://config.uca.cloud.unity3d.com • http://chilliant.blogspot.com.au/2012/08/srgb-aG • https://perf-events.cloud.unity3d.com • http://www.ascendercorp.com/typedesigners.html • http://www.ascendercorp.com • https://api.uca.cloud.unity3d.com/v1/events • https://lineto.com/licensinghttps • https://kokua-backend.tripp.com • https://us-central1-tripp-dev.cloudfunctions.net • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/8 • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/54 • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/65 • http://scripts.sil.org/OFL	自研引擎-A
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1lSDK.java
• https://iamcache.braze/ab_triggers	com/braze/support/WebContentUtils.java
• https://sdk.iad-01.braze.com/api/v3/ • https://sondheim.braze.com/api/v3/	com/braze/configuration/BrazeConfigurationProvider.java
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1fSDK.java
• https://www.braze.com/docs/user_guide/administrative/access_braze/sdk_endpoints • https://www.braze.com/docs/developer_guide/platform_integration_guides/android/initial_sdk_setup/android_sdk_integration/	com/braze/Braze.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://iamcache.braze/	com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java
• https://%sonelink.%s/shortlink-sdk/v2 • https://%sgcdsdk.%s/install_data/v5.0/ • https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id=	com/appsflyer/internal/AFe1sSDK.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1cSDK.java

• https://mobile.events.data.microsoft.com/onecollector/1.0	com/microsoft/appcenter/ingestion/OneCollectorIngestion.java
• https://in.appcenter.ms	com/microsoft/appcenter/ingestion/AppCenterIngestion.java
• https://dust.k8s.test-001.d-usw-2.braze.com/sse?mite=	com/braze/managers/y.java
• https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%svalidate.%s/api/v • https://%sconversions.%s/api/v • https://aps-webhandler.appsflyer.com/api/trigger • https://%slaunches.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.15.0/android?app_id= • https://%ssdk-services.%s/validate-android-signature • https://%sinapps.%s/api/v • https://%sattr.%s/api/v	com/appsflyer/internal/AFj1mSDK.java
• https://%sapp.%s	com/appsflyer/internal/AFj1gSDK.java
• https://tripp-prod.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://tripp-prod.firebaseio.com 的Firebase 数据库进行通信

		Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/626950017386/namespaces/firebase:fetch?key=AIzaSyDQQpFJCvlFk4g_5FM_2xDWGTN_7PXl3UA ） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		
		{
		"entries": {
		"app_rating_day": "9",
		"app_rating_feature_enabled": "true",
		"blacklisted_versions_android": "",
		"blacklisted_versions_ios": "",
		"demo_user_email": "tripp_seat+anonymous@trippinc.com",
		"demo_user_pwd_encrypted": "BnSEGwmkHVpCFlqf7CeSjg==",
		"instant_analytic_events": "MobileAppSignUp;MobileAppLogin;MobileAppLogout;MobileAppLaunched;CompanionDeviceInstallation;MobileKokuaRunStarted;MobileKokuaInputScreenClosed;MobileKokua1stInputScreenCompleted;MobileKokuaMeditationStarted;MobileKokuaMeditationSkipped;MobileKokuaMeditationCompleted;MobileKokua2ndInputScreenCompleted;MobileKokuaContentRatingStarted;MobileKokuaContentRatingSkipped;MobileKokuaContentRatingCompleted;MobileKokuaFeatureRatingStarted;MobileKokuaFeatureRatingSkipped;MobileKokuaFeatureRatingCompleted;MobileKokuaShareButtonPressed;MobileKokuaPinEntryScreenEntered;MobileKokuaRunEnded;XrKokuaEstablishConnectionWaitTime;XrKokuaKeyboardInputSent;XrKokuaInterrupt;TrippMicPermissionState;XrKokuaCaptionsEnabled;XrKokuaCaptionsDisabled;XrKokuaReflectionStarted;XrKokuaReflectionCompleted;XrKokuaUserRespondedPostReflection;XrKokuaReflectionPoolImageGenerationSucceded;XrKokuaReflectionPoolImageGenerationFailed;CompanionSubmitPhoto;CompanionRejectPhoto;MobileWeeklyStreak1;MobileWeeklyStreak2;MobileWeeklyStreak3;MobileWeeklyStreak4;MobileWeeklyStreak5;MobileWeeklyStreak6;MobileWeeklyStreak7;MobileIAPInitializationEvent;MobileIAPPurchaseStartedEvent;MobileIAPPurchaseFinishedEvent;MobileIAPPurchaseFailedEvent;MobilePreviousPurchaseDetected;MobileWelcomeScreenOnboardingFunnel;MobileSurveyStartedOnboardingFunnel;MobileSurveySubmittedOnboardin

Firebase远程配置已启用	警告	gFunnel;MobileSurveySkippedOnboardingFunnel;MobileSubscriptionPlansEnteredOnboardingFunnel;MobileSubscriptionPlansSkippedOnboardingFunnel;MobileSubscriptionPurchaseStartedOnboardingFunnel;MobileSubscriptionPurchaseSucceededOnboardingFunnel;MobileSubscriptionPurchaseFailedOnboardingFunnel;MobileSubscriptionPlansEnteredGateFunnel;MobileSubscriptionPlansSkippedGateFunnel;MobileSubscriptionPurchaseStartedGateFunnel;MobileSubscriptionPurchaseSucceededGateFunnel;MobileSubscriptionPurchaseFailedGateFunnel;MobileSubscriptionUpsellVrEnteredGateFunnel;MobileSubscriptionComparisonEnteredGateFunnel;MobileJoinForkFunnel;MobileUseVrForkFunnel;MobileLoginForkFunnel;MobileCreateAccountMobileStartedOnboardingFunnel;MobilePairDeviceVrIntroEnteredOnboardingFunnel;MobileCreateAccountVrStartedOnboardingFunnel;MobileCreateAccountMobileCompletedOnboardingFunnel;MobileCreateAccountVrCompletedOnboardingFunnel;MobilePairDeviceVrEnteredOnboardingFunnel;MobilePairDeviceVrSkippedOnboardingFunnel;MobilePairDeviceVrSucceededOnboardingFunnel;MobilePromotionsDeeplinkScreenOpened;MobilePromotionsDeeplinkScreenPurchaseInitiated;MobilePromotionsDeeplinkScreenPurchaseSucceeded;MobilePromotionsDeeplinkScreenPurchaseFailed", "kokua_create_for_others_flow_enabled": "true", "kokua_entry_enabled": "true", "kokua_feature_enabled": "true", "kokua_image_generation_enabled": "true", "kokua_voice_cloning_enabled": "false", "minimal_version_android": "1.15.9", "minimal_version_ios": "1.15.9", "recommended_version_android": "1.15.10", "recommended_version_ios": "1.15.10", "weekly_goals_bonus_aura": "10", "weekly_goals_data": "[{\"GoalTitle\": \"Check-in with Yourself\",\"GoalDescription\": \"Track mood {0} days this week\",\"WeeklyGoalType\":2,\"RequiredCountToComplete\":[3],\"AuraRewardAmount\":3,\"MaxCompletionPerDay\":1},{\"GoalTitle\": \"Get Support from Kōkua\",\"GoalDescription\": \"Chat with Kōkua {0} days this week\",\"WeeklyGoalType\":0,\"RequiredCountToComplete\":[2],\"AuraRewardAmount\":3,\"MaxCompletionPerDay\":1},{\"GoalTitle\": \"Expand your Practice\",\"GoalDescription\": \"Listen to TRIPP of the week\",\"WeeklyGoalType\":4,\"RequiredCountToComplete\":[1],\"AuraRewardAmount\":3,\"MaxCompletionPerDay\":1}]", "weekly_goals_enabled": "true", "weekly_goals_featured_audio_content_playlist_id": "3c3cab0b8528a768fe562676169e8c72" }, "state": "UPDATE", "templateVersion": "60"

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。

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。

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 CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

敏感凭证泄露检测

可能的密钥
"PASSWORD" : "Password"
"USERNAME" : "Username"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"appcenter_app_secret" : "8e4f9af1-a53a-4216-a0c3-356dbbf9bd60"
"com.google.firebase.crashlytics.unity_version" : "2020.3.47f1"
"com_braze_api_key" : "7ec70f34-be63-4e9b-ab76-fe4d1e1e5777"
"com_braze_firebase_cloud_messaging_sender_id" : "626950017386"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"com_braze_inapp_initial_display_operation_key" : "DISPLAY_NOW"
"enable_manual_session_tracker" : "False"
"firebase_database_url" : "https://tripp-prod.firebaseio.com"

"google_api_key" : "AIzaSyDQQpFJCvlFk4g_5FM_2xDWGTN_7PXl3UA"
"google_app_id" : "1:626950017386:android:a02b5159070594a7"
"google_crash_reporting_api_key" : "AIzaSyDQQpFJCvlFk4g_5FM_2xDWGTN_7PXl3UA"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasenya"
"PASSWORD" : "Adgangskode"
"USERNAME" : "Brugernavn"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Adgangskode"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passord"
"PASSWORD" : "Passwort"
"USERNAME" : "Nutzername"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passwort"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wagwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Wagwoordsleutel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Salasana"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Avainkoodi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasinal"
"PASSWORD" : "Wachtwoord"
"USERNAME" : "Gebruikersnaam"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wachtwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Toegangssleutel"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Klucz"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Geslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Sandi"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Zaporka"

"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parool"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"PASSWORD" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Pasahitza"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Sarbide-gakoa"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Iphasiwedi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parole"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Nyckel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Nenosiri"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Kod"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Palavra-passe"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
37a6259cc0c1dae299a7866489dff0bd

FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

Google Play 应用市场信息

标题: TRIPP: Calm Focus Sleep Ascend

评分: 4.62 **安装:** 50,000+ **价格:** 0 **Android版本支持:** **分类:** 健康与健身 **Play Store URL:** com.tripp.companion

开发者信息: TRIPP Inc., 5457631680582396493, None, https://www.tripp.com, support@tripp.com,

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

关于此应用:

TRIPP：提升您的心灵。 转变始于 TRIPP，这款应用程序将人工智能心理健康教练放在您的口袋里。 TRIPP 利用经过数百万次人际互动训练的人工智能，提供量身定制的体验，以提升您的思维清晰度、促进放松并支持您的全面成长。无论您是寻求更专注的专注力、压力管理，还是日常健康的工具，TRIPP 都能为您提供一条通往更健康的动态之路。享受睡眠故事、自然声音、双耳频率、屡获殊荣的音乐、受人尊敬的冥想导师等等。 认识 Kōkua：您的人工智能健康指南 Kōkua 是您的个性化人工智能指南，旨在通过主动指导和洞察来支持您的健康之旅。通过互动指导和定制反思，Kōkua 帮助您应对日常挑战、培养积极习惯并实现您的健康目标。与 Kōkua 互动，深入了解自己，并制定持久健康的策略。 与您的社区分享支持 通过与您的朋友、家人和网络分享振奋人心的信息和健康鼓励，扩大 TRIPP 的积极影响。支持他人追求以心为本的生活，并培养积极的文化。 TRIPP 助您重塑现实。 TRIPP 移动高级版订阅 您可以订阅 TRIPP 移动高级版，并从以下方案中选择： • 1 个月 • 12 个月（新订阅者可享受 7 天免费试用）。当您确认首次订阅购买时，款项将从您 Google Play 帐户关联的信用卡中扣除。除非在当前订阅期结束前至少 24 小时关闭自动续订，否则您的订阅将自动续订。您可以在购买后在 Google Play 帐户设置中关闭自动续订。免费试用期的任何未使用部分（如有提供）将在您购买订阅时作废（如适用）。 点击此处了解更多我们的条款和条件：服务条款：https://www.tripp.com/terms-of-service 隐私政策：https://www.tripp.com/privacy-policy

---

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。