南明离火
移动应用检测平台

ANDROID 静态分析报告

Kahramaa • v15.23.3

分析日期: 2025-08-26 20:54:24

应用概览

文件名称:	Kahramaa v15.23.3.apk
文件大小:	15.02MB
应用名称:	Kahramaa
软件包名:	com.vipera.dynamicengine
主活动:	com.qa.kahramaa.kahramaa.splash.SplashActivity
版本号:	15.23.3
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:	63/100 (低风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	e7704e1933b5227d8a292ae3d0ac9268
SHA1:	2a07ba0a7e155b063ca2fa6ef1cc276c31c59730
SHA256:	be4d56ce362a04a4a12771b2426763f1666fbfe8804fbc8d032c67976bd0faf2

分析结果严重性分布

高危	中危	信息	安全	关注
1	12	2	4	0

四大组件导出状态统计

Activity组件：6个，其中export的有： 0个
Service组件：10个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：3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: L=doha, OU=kahramaa, CN=Kahramaa
签名算法: rsassa_pkcs1v15
有效期自: 2014-02-27 13:50:30+00:00
有效期至: 2039-02-21 13:50:30+00:00
发行人: L=doha, OU=kahramaa, CN=Kahramaa
序列号: 0x6bee1ed4
哈希算法: sha256
证书MD5: a6a21e46b6b2d490776daf9b4c95f796
证书SHA1: a0ed9cc9cd711a66bfb6ac4f88917e5f496ad4ba
证书SHA256: 13a76d821af499e85a7d4a5a7706349b5b31d13f96fc2fb64d43178ffefcd560
证书SHA512:
f7da208657e99d7f2eb4dd7bb83969078fec4509fe160b6ab7975b6bb024382ba21955c519f69e7ce8cdc2a84258a43ef1e0d832abc681f4f26c0de13619fb7e

公钥算法: rsa
密钥长度: 2048
指纹: e5d9ba9afa08d91e74c7c6a9d59ea992e802d15eeff2a0bf9cc9590c393980b4
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.LOCATION_HARDWARE	普通	允许使用硬件中的定位功能	允许应用程序在硬件中使用位置功能，例如：geofencing api。
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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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。
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.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.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.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.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
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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，甚至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.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.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。

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: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F120001]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	Service (com.firebase.jobdispatcher.GooglePlayReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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。
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	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: **1** | 警告: **7** | 信息: **1** | 安全: **3** | 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
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

本报告由南明离火移动安全分析平台生成

4	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
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	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	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
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	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
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	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

12	此应用程序使用Safety Net API。	安全	OWASP MASVS: MST G-RESILIENCE-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
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
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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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
00013	读取文件并将其放入流中	文件	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
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
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
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
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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00131	获取当前GSM的位置并将其放入JSON中	信息收集 位置	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
00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	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
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	升级会员：解锁高级权限

00099	获取当前GSM的位置并将其放入JSON中	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
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
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
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 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
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
00121	创建目录	文件 命令	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
00046	方法反射	反射	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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 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
00075	获取设备的位置	信息收集 位置	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
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
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
00014	将文件读入流并将其放入 JSON 对象中	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

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
00147	获取当前位置的时间	信息收集 位置	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

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.RECEIVE_BOOT_COMPLETED android.permission.CAMERA android.permission.WAKE_LOCK
其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.READ_MEDIA_IMAGES com.google.android.c2dm.permission.RECEIVE 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
kiosk.km.qa	安全	否	No Geolocation information available.
instagram.com	安全	否	**IP地址:** 31.13.70.174 **国家:** 美国 **地区:** 美国加利福尼亚州 **城市:** 洛杉矶 **纬度:** 34.0522342 **经度:** -118.2436849 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.176.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

mprd.km.qa	安全	否	**IP地址:** 5.180.36.6 **国家:** 卡塔尔 **地区:** 阿达瓦 **城市:** 多哈 **纬度:** 25.279720 **经度:** 51.522449 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.151.33 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
apps.km.qa	安全	否	**IP地址:** 5.180.36.65 **国家:** 卡塔尔 **地区:** 阿达瓦 **城市:** 多哈 **纬度:** 25.279720 **经度:** 51.522449 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **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
km.qa	安全	否	**IP地址:** 5.180.36.62 **国家:** 卡塔尔 **地区:** 阿达瓦 **城市:** 多哈 **纬度:** 25.279720 **经度:** 51.522449 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
api.whatsapp.com	安全	否	**IP地址:** 31.13.70.49 **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

kahramaa-14fd8.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
api.ipify.org	安全	否	**IP地址:** 104.26.12.205 **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://cdn.euc-freshbots.ai/assets/share/js/freshbots.min.js	自研引擎-A
• https://kiosk.km.qa/terms/ • https://kiosk.km.qa/terms/en.html	com/qa/kahramaa/kahramaa/login/fragments/RegistrationInitiateFragment.java
• https://mprd.km.qa/cstservices/service.svc/ • https://mprd.km.qa/kmservices/ • https://mprd.km.qa/ptservices/	com/qa/kahramaa/kahramaa/base/retrofit/WebServiceFactoryV2.java
• http://instagram.com/_u/kahramaa • https://api.whatsapp.com/send?phone=+97430303991 • https://twitter.com/#!/kahramaa • https://www.facebook.com/kahramaa/ • https://www.facebook.com/kahramaa	com/qa/kahramaa/kahramaa/home/fragments/HomeFragment.java
• https://play.google.com/store/apps/details?id=	oc/v.java
• https://drive.google.com/viewerng/viewer?embedded=true&url=https://www.km.com.qa/customerservice/documents/termsandconditions.pdf	gc/n1.java
• https://play.google.com/store/apps/details?id=	oc/r.java
• https://play.google.com/store/apps/details?id=	oc/k.java
• https://play.google.com/store/apps/details?id=	oc/e0.java
• http://docs.google.com/gview?embedded=true&url=https://www.km.com.qa/consultant/documents/mfsd-fcs-16-01.pdf	com/qa/kahramaa/kahramaa/ezab/fragments/EzabRequestFragment.java
• https://km.qa/pages/faqs.aspx?openinmobileapp=1 • https://api.whatsapp.com/send?phone=+97430303991	com/qa/kahramaa/kahramaa/home/fragments/SupportFragmentNewUI.java
• https://play.google.com/store/apps/details?id=com.google.android.apps.docs.editors.docs	nb/x.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	b5/b.java

• https://app-measurement.com/a	r6/d0.java
• https://kiosk.km.qa/terms/ • https://kiosk.km.qa/terms/en.html	com/qa/kahramaa/kahramaa/settings/fragments/SettingsFragment.java
• https://app-measurement.com/a	g6/la.java
• https://km.qa/pages/faqs.aspx?openinmobileapp=1 • https://kiosk.km.qa/terms/ • https://kiosk.km.qa/terms/en.html	com/qa/kahramaa/kahramaa/settings/fragments/LinkFragment.java
• https://firebase.google.com/support/privacy/init-options	v9/d.java
• https://apps.km.qa/billlist/	com/qa/kahramaa/kahramaa/base/activities/MainActivity.java
• https://api.whatsapp.com/send?phone=+97430303991	com/qa/kahramaa/kahramaa/home/fragments/HomeFragmentNewUI.java
• https://play.google.com/store/apps/details?id=com.google.android.apps.docs.editors.docs	nb/y.java
• www.google.com • https://www.google.com • https://goo.gl/naoooi	r6/u9.java
• www.cancelprofiling • www.get	com/threatmetrix/TrustDefender/RL/uuuhhu.java
• https://%s/%s/%s	y9/c.java
• https://api.ipify.org/	com/qa/kahramaa/kahramaa/partialpayment/fragments/GooglePayUsersDetail.java
• https://kiosk.km.qa/terms/ • https://kiosk.km.qa/terms/en.html	com/qa/kahramaa/kahramaa/login/fragments/KmRegistration.java
• https://kahramaa-14fd8.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://kahramaa-14fd8.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/588504448995/namespaces/firebase:fetch?key=AIzaSyAdBg5I0Ld8J9iGX32l1mx6TH3_TEwWo-U ） 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 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 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。

邮箱地址敏感信息提取

EMAIL	源码文件
customercare@km.qa	com/qa/kahramaa/kahramaa/home/fragments/HomeFragment.java
customercare@km.qa	com/qa/kahramaa/kahramaa/settings/fragments/SettingsFragment.java
customercare@km.qa	com/qa/kahramaa/kahramaa/home/fragments/HomeFragmentNewUI.java

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
凭证信息=> "com.google.android.geo.API_KEY" : "@7F0F0001"
"API_KEY_FABRIC" : "fb9320e5869d965fc717c4bbc96174424f91d674"
"API_KEY_G_MAP" : "AIzaSyDqeqdDLSYe-UDED9TxKk_SaX7OwpPnwKA"
"firebase_database_url" : "https://kahramaa-14fd8.firebaseio.com"

"google_api_key" : "AIzaSyAdBg5I0Ld8J9iGX32l1mx6TH3_TEwWo-U"
"google_app_id" : "1:588504448995:android:a741ecd69459ad8d"
"google_crash_reporting_api_key" : "AIzaSyAdBg5I0Ld8J9iGX32l1mx6TH3_TEwWo-U"
"max_limit_reached_api" : "api"
"password" : "Password"
"reached_api_max_limit" : "reached_api_max_limit"
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472600882589380018616069731[illegible]319
39402006196394479212279040100143613805079739270465446667946905279627659399113263569898956308152294913554[illegible]33653942643
6864797660130609714981900799081393217269435300143305409394463459185543183[illegible]97056052422559640661454654977296311391480858037121987999716643812574028291115057151
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b[illegible]e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
1157920892103562487626974469494075735299969552241357603[illegible]4122590610685120443[illegible]69
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141126314088f5013875ac656398d8a2e[illegible]19d2[illegible]85c8edd3ec2aef
470fa2b4ae81cd56ecbcda9735803434cec591fa
051953eb9618e1c9a1f929a21a0b68540eea2[illegible]5b99b315f3b8b489918e[illegible]09a156[illegible]93951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
11839296a789a3bc0045c8a5fb42c7d7ac9[illegible]54449579b446817af5d[illegible]73e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372807[illegible]005449
aa87ca22be8b[illegible]eb1c71ef320ad746e[illegible]b[illegible]b[illegible]79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735300861434152903141955336313088670978539[illegible]51
5ac635d8aa3a93e7b3ebbd557[illegible]bc651d06b0cc53b0f63bce3c3e27d2604b

Google Play 应用市场信息

标题: Kahramaa

评分: 4.706897 安装: 100,000+ 价格: 0 **Android**版本支持: 分类: 办公 **Play Store URL:** com.vipera.dynamicengine

开发者信息: Qatar General Electricity & Water Corporation, Qatar+General+Electricity+%26+Water+Corporation, None, https://km.qa, contactus@km.qa,

发布日期: 2014年2月27日 **隐私政策:** Privacy link

关于此应用:

卡塔尔通用电力和水务公司的官方应用程序 “Kahramaa”为客户提供以下几种电子服务： - 查看和支付电费和水费 - 我的物业服务 - 电子表格服务 - 服务状态追踪 - 更新电子账单电子邮件 - 提交抄表 - 证书申请 - 在地图上找到客户服务分支机构 - 向 Kahramaa 发送建议或投诉，如有需要，附上图片

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。