南明离火
移动应用检测平台

ANDROID 静态分析报告

Kapu Sangam • v2.8.1

分析日期: 2025-03-11 14:20:46

应用概览

文件名称:	com-sangam-kapu-36-63914594-eafe6c97aa02f2147a210e358e703b8f.apk
文件大小:	3.28MB
应用名称:	Kapu Sangam
软件包名:	com.sangam.kapu
主活动:	com.communityshaadi.android.ui.splash.SplashActivity
版本号:	2.8.1
最小SDK:	17
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	4/432
杀软检测:	经检测，该文件安全
MD5:	eafe6c97aa02f2147a210e358e703b8f
SHA1:	f79e092fb341bcbeaa3a2c9190dbaa64d09d9f12
SHA256:	160fd34763d52087d39e3c4546afc9cc95477fea7c37f01f55d577e91083e46f

分析结果严重性

高危	中危	信息	安全	关注
6	19	3	3	2

四大组件信息

Activity组件：7个，其中export的有： 1个
Service组件：13个，其中export的有： 4个
Receiver组件：1个，其中export的有： 2个
Provider组件：4个，其中export的有： 0个

证书信息

二进制文件已签名
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: 2019-03-18 11:27:37+00:00
有效期至: 2049-03-18 11:27:37+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xc340da44ae54cbbbe561ed321485c6f9fcae561d
哈希算法: sha256
证书MD5: 31f908108d8887d1f8913feeac4a020e
证书SHA1: a04d2dec5a81f6bdc2e02dd8f7ae21f03af32612
证书SHA256: 739f27aac97af95f0839e68776c9f507bda71dc04d8895658331c6b265bfb4ae
证书SHA512:
966a8d90fb367d95a511d523cc2818e1247f94348a42995fd5c7f8af4e9187b4a0cdbe0a53045a66dd02f739586b54ea02df410792fc3dde34e4e39fd21ab01f

公钥算法: rsa
密钥长度: 4096
指纹: cd345534d3849f58e0c8532c730607534611623a6e0f13bc0933bb909ed21749
找到 1 个唯一证书

应用权限

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_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_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.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。
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.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.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.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.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。

可浏览的Activity组件

ACTIVITY	INTENT

com.communityshaadi.android.ui.main.MainActivity	Schemes: http://, https://, Hosts: sd2.in, *.sangam.com, Path Prefixes: /,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **5** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	App 链接 assetlinks.json 文件未找到 [android:name=com.communityshaadi.android.ui.main.MainActivity] [android:host=http://sd2.in]	高危	App Link 资产验证 URL （http://sd2.in/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：301）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify=“true”] 启用验证来验证 App Link 网域。
3	App 链接 assetlinks.json 文件未找到 [android:name=com.communityshaadi.android.ui.main.MainActivity] [android:host=http://sangam.com]	高危	App Link 资产验证 URL （http://sangam.com/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：301）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify=“true”] 启用验证来验证 App Link 网域。
4	App 链接 assetlinks.json 文件未找到 [android:name=com.communityshaadi.android.ui.main.MainActivity] [android:host=https://sangam.com]	高危	App Link 资产验证 URL （https://sangam.com/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：301）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify=“true”] 启用验证来验证 App Link 网域。
5	Activity (com.communityshaadi.android.ui.main.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

6	Activity (com.communityshaadi.android.ui.main.MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
7	Service (com.communityshaadi.android.service.fcm.FcmService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
8	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
11	Activity (com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
12	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
13	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

</> 安全漏洞检测

高危: **1** | 警告: **9** | 信息: **2** | 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	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
3	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
4	该文件是World Writable。任何应用程序都可以写入文件	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
5	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
6	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
7	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
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	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
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

11	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
12	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
13	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
14	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

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
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
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
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
00091	从广播中检索数据	信息收集	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
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
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
00092	发送广播	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
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
00153	通过 HTTP 发送二进制数据	http	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
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
00036	从 res/raw 目录获取资源文件	反射	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
00191	获取短信收件箱中的消息	短信	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
00075	获取设备的位置	信息收集 位置	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
00113	获取位置并将其放入 JSON	信息收集 位置	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
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
00012	读取数据并放入缓冲区	文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.c2dm.permission.RECEIVE

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。

域名检测

域名	状态	中国境内	位置信息
sattr.s	安全	否	No Geolocation information available.
kapu.sangam.com	安全	否	**IP地址:** 104.18.28.214 **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
pagead2.googlesyndication.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:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
sonelink.s	安全	否	No Geolocation information available.
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:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
simpression.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.

goo.gl	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
app-notify-b79ce.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
sinapps.s	安全	否	No Geolocation information available.
sstats.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• https://%svalidate.%s/api/v4.11/androidevent?buildnumber=5.0.0&app_id= • https://%ssdk-services.%s/validate-android-signature	com/appsflyer/internal/y.java
• https://app-measurement.com/a	b/b/a/d/g/i/r9.java
• javascript:onotprecieved • https://kapu.sangam.com/	com/communityshaadi/android/ui/main/MainActivity.java
• https://%sregister.%s/api/v4.11/androidevent?buildnumber=5.0.0&app_id=	com/appsflyer/internal/ab.java
• https://%sonelink.%s/shortlink-sdk/v1	com/appsflyer/internal/ad.java
• https://%sstats.%s/stats • https://%smonitorsdk.%s/remote-debug?app_id=	com/appsflyer/internal/g.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	b/b/a/d/a/a/b.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%sregister.%s/api/v4.11/androidevent?buildnumber=5.0.0&app_id= • https://%sgcdsdk.%s/install_data/v4.0/ • https://%sattr.%s/api/v4.11/androidevent?app_id= • https://%sconversions.%s/api/v4.11/androidevent?app_id= • https://%slaunches.%s/api/v4.11/androidevent?app_id= • https://%sinapps.%s/api/v4.11/androidevent?app_id=	com/appsflyer/AppsFlyerLibCore.java

• https://%sapp.%s	com/appsflyer/share/Constants.java
• https://%sonelink.%s/shortlink-sdk/v1	com/appsflyer/CreateOneLinkHttpTask.java
• https://goo.gl/j1swqy	b/b/a/d/g/i/g0.java
• https://app-notify-b79ce.firebaseio.com	自研引擎-S

FIREBASE数据库分析

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://app-notify-b79ce.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/844867688/namespaces/firebase:fetch?key=AIzaSyDPGlaCRYR18-4-[redacted]tEpNClMi4aftW6g ） 已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

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。
Dexter	Karumi	Dexter 是一个 Android 库，它简化了运行时请求权限的过程。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 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。
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。

追踪器

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
Snowplow	Analytics	https://reports.exodus-privacy.eu.org/trackers/108

密钥凭证

可能的密钥
"firebase_database_url" : "https://app-notify-b79ce.firebaseio.com"
"google_api_key" : "AIzaSyDPGlaCRYR18-4-ZY93tEpIClMi4aftW6g"
"google_app_id" : "1:886044867688:android:c466c67ec5286188"
"google_crash_reporting_api_key" : "AIzaSyDPGlaCRYR18-4-ZY93tEpIClMi4aftW6g"

GooglePlay应用信息

标题: Kapu Matrimony App by Sangam

评分: 4.2222223 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 社交 **Play Store URL:** com.sangam.kapu

开发者信息: People Interactive, People+Interactive, None, https://kapu.sangam.com/, care@sangam.com,

发布日期: 2019年3月18日 **隐私政策:** Privacy link

关于此应用:

值得信赖的卡普婚姻应用程序用于婚介 欢迎来到 Kapu Sangam，这是寻找 Kapu 新娘/新郎的最古老的家庭婚介服务之一。 印度的婚姻关系到家庭和社区——而不仅仅是两个人。我们的应用程序是从头开始创建的，牢记这一现实。 我们始终通过创新和消费者至上的方法使自己与其他服务区分开来，旨在让您在找到合适的伴侣和家庭时感到安全、可靠、放心、联系和舒适。这使您可以简单轻松地搜索您周围符合条件的新娘/新郎的 Kapu 婚姻资料。 我们的应用程序采用直观的方法，引导您顺利完成注册过程，并让您立即与志同道合的 Kapu 家庭互动。 为什么选择 Kapu Sangam 应用程序进行婚姻搜索？ 凭借超过 10 万份个人资料和超过 50,000 个成功案例，我们正迅速成为全球卡普家庭值得信赖的卡普婚姻和婚介服务机构之一。平台功能包括： - 政府验证的用户资料 - 每个用户都必须有个人资料照片 - 昆达利匹配功能 - 无限的个人资料和匹配 - 详细的家庭信息 - 仅限卡普家庭比赛 我们的过滤系统力求只显示那些与您相关的匹配项。 作为值得信赖的婚介和卡普婚姻应用程序之一，我们不断以创新方式改变的方法重新定义界限。我们知道婚姻是个人一生中最重要的里程碑，也是家庭中的重要时刻。因此，我们让您可以简单轻松地搜索您周围符合条件的卡普新娘/新郎的婚姻档案，并获取有关他们家庭的所需信息。 以下是有关如何更有效地使用该应用程序的一些提示： - 注册并创建您的婚姻档案并仅查找高级专属档案 - 查看您的匹配对象的完整档案以及他们的照片和家庭信息 - 根据您的喜好和家人的喜好选择适合的比赛 使用我们的应用程序，您不仅可以为自己创建 Kapu 婚姻档案，而且如果您是父母、兄弟姐妹、叔叔、阿姨或祖父母，您还可以代表您所爱的人注册。 配对从未如此简单，您可以： - 查看您想要联系的婚姻档案的电话号码和电子邮件 ID - 发送个性化消息并与您入围的卡普婚姻档案发起聊天 - 提高您婚姻档案的可见度和回应 按位置搜索卡普婚姻资料：通过我们的位置过滤功能，您可以知道准新娘/新郎的家庭所在位置，并且您在社区内的联系将比以往任何时候都更加紧密。 使用此应用程序，您可以搜索海得拉巴、钦奈、班加罗尔、孟买、维杰亚瓦达或班加罗尔（班加罗尔）等主要城市的婚姻档案。 按首选社区查找个人资料 配对是将两个人和他们的家人配对在一起的过程，我们知道找到一个社区找到匹配对象对您来说有多重要。因此，我们让您可以轻松搜索 Kamma、Kapu、Balija、Gavara、Golla 等主要社区的个人资料。我们致力于确保我们平台上发布的每一份婚姻资料都经过筛选，为您提供安全的体验。我们是值得信赖的卡普婚介服务公司之一，拥有真正认真对待婚姻的人的真实资料。 因此，是时候下载 Kapu Sangam 应用程序、创建您的个人资料并离您完美的生活伴侣更近了一步。

免责声明及风险提示: