



ANDROID 静态分析报告



◆ Lovemix • v1.0.8

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-03-11 14:30:15

i应用概览

文件名称:	Lovemix v1.0.8.apk
文件大小:	3.97MB
应用名称:	Lovemix
软件包名:	com.lovemix
主活动:	com.euromatch.lovemix.MainActivity
版本号:	1.0.8
最小SDK:	23
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	56/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测, 该文件安全
MD5:	0399ebab09ccb363846ac6bb78e93115
SHA1:	4e6fba930ebd770d590082c1f3c3ceb5d573953a
SHA256:	9194c6d47c0839dccc7afb73c004f4d8cc8c8e2d3a3d9527338a4ad500930a828

分析结果严重性

高危	中危	信息	安全	关注
0	10	2	1	0

四大组件信息

Activity组件: 5个, 其中export的有: 0个
Service组件: 8个, 其中export的有: 1个
Receiver组件: 4个, 其中export的有: 1个
Provider组件: 3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: 2020-02-14 16:51:57+00:00

有效期至: 2050-02-14 16:51:57+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0xa1a934b7a1d383477b7b7763f43c6fa71af81ab3

哈希算法: sha256

证书MD5: 549b636b86e88e7366f2978f96a32a9c

证书SHA1: ad91111dbef9f280a5ca85bd169209c8f33156630

证书SHA256: ca5cad7a95689488ba424460388db5760d3733440d12dfd24704f53b8c87c0a0

证书SHA512:

f08e1ba6d949a07c84adb02f1d23783a35b7287b7c753d0e883f58c965ce0ca3cf9db3eed66163bc7cf9b182bd0e8fa7893b70f8debf1c82447b3b4fca1de579d

公钥算法: rsa

密钥长度: 4096

指纹: fdd927edefd11a8dd8cfa8a9e384e4f7b8b1e1c4036e04f4ab84266aa67b626b

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.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_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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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。
com.google.android.finsky.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.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.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.POST_NOTIFICATIONS	危险	发送通知的运行时代权限	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，在手机屏幕关闭后后台进程仍然运行。
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.lovemix.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
--	----	------	---------------------

可浏览的Activity组件

ACTIVITY	INTENT
com.euromatch.lovemix.MainActivity	Schemes: https://, lovemix://, Hosts: www.lovemix.com, lovemix.co.uk, www.placere.ro, Path Prefixes: /app,

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: 0 | 警告: 3 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
2	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。
3	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: 0 | 警告: 5 | 信息: 1 | 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: MST G-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: MST G-CRYPTO-6	升级会员: 解锁高级权限
3	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: MST G-STORAGE-2	升级会员: 解锁高级权限
4	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: MST G-STORAGE-2	升级会员: 解锁高级权限
5	不安全的WebView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: MST G-PLATFORM-7	升级会员: 解锁高级权限
6	可能存在跨域漏洞。在WebView中启用从URL访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MST G-PLATFORM-7	升级会员: 解锁高级权限

行为分析

编号	行为	标签	文件
00208	捕获设备屏幕的内容	信息收集 屏幕	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
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
00091	从清单中检索数据	信息收集	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
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

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
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
00013	读取文件并将其放入流中	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
00194	设置音源 (MIC) 和录制文件格式	录制音视频	升级会员: 解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员: 解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员: 解锁高级权限
00056	修改语音音量	控制	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	5/30	android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.FOREGROUND_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。

域名检测

域名	状态	中国境内	位置信息
lovemix.co.uk	安全	否	IP地址: 54.37.196.148 国家: 德国 地区: 黑森 城市: 林堡 纬度: 50.383598 经度: 8.050300 查看: Google 地图

www.placere.ro	安全	否	IP地址: 54.37.196.148 国家: 德国 地区: 黑森 城市: 林堡 纬度: 50.383598 经度: 8.050300 查看: Google 地图
lovemix-bf317.firebaseio.com	安全	否	IP地址: 54.37.196.148 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
www.lovemix.com	安全	否	IP地址: 54.37.196.148 国家: 德国 地区: 黑森 城市: 林堡 纬度: 50.383598 经度: 8.050300 查看: Google 地图
www.lovemix.co.uk	安全	否	IP地址: 54.37.196.148 国家: 德国 地区: 黑森 城市: 林堡 纬度: 50.383598 经度: 8.050300 查看: Google 地图

🌐 URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://www.lovemix.com/members/upgrade? https://play.google.com/store/apps/details?id= https://www.placere.ro https://www.lovemix.com/members/home https://www.lovemix.com https://www.lovemix.com/app/installed https://www.lovemix.com/members/upgrade?latest& https://www.lovemix.co.uk https://www.lovemix.com/upgrade-redirect/ https://lovemix.co.uk 	com/euromatch/lovemix/MainActivity.java
<ul style="list-style-type: none"> https://lovemix-bf317.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://lovemix-bf317.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	<p>Firebase远程配置URL (https://firebaseremoteconfig.googleapis.com/v1/projects/812653253775/namespaces/firebase:fetch?key=AlzaSyC6F1P83kfdmx_1Gi-uxLuHa12PRaT_y5c) 已禁用。响应内容如下所示:</p> <pre>{ "state": "NO_TEMPLATE" }</pre>
-----------------	----	--

第三方SDK

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 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、高效的方法在应用程序启动时初始化组件。库开发人员 and 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。
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 and newer API versions of the platform (many using Material Design)

追踪器

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
"facebook_app_id" : "189150061276493"
"firebase_database_url" : "https://lovemix-bf317.firebaseio.com"
"google_api_key" : "AlzaSyC6F1P83kfdmx_1Gi-uxLuHa12PRaT_y5c"
"google_app_id" : "1:812653253775:android:fa753f67fbda3a68f84cfa"
"google_crash_reporting_api_key" : "AlzaSyC6F1P83kfdmx_1Gi-uxLuHa12PRaT_y5c"

c06c8400-8e06-11e0-9cb6-0002a5d5c51b

0123456789qwertyuiopasdfghjklzxcvbnm

bb392ec0-8d4d-11e0-a896-0002a5d5c51b

GooglePlay应用信息

标题: Lovemix: Chat, Friends, Hookup

评分: 4.3846154 **安装:** 50,000+ **价格:** 0 **Android版本支持:** **分类:** 约会交友 **Play Store URL:** [com.lovemix](https://play.google.com/store/apps/details?id=com.lovemix)

开发者信息: Lovemix, Lovemix, Lootsa tn 5 // Sepapaja tn 4 Tallinn, Harjumaa, 11415, <https://www.lovemix.com>, contact@lovemix.com,

发布日期: 2020年10月22日 **隐私政策:** [Privacy link](#)

关于此应用:

Lovemix 是一个约会社区, 在这里您可以结识真正的、志同道合、对社交感兴趣的人。□□日常搭配 从出去喝咖啡到欣赏的人一起看日出。与有兴趣加入您或您自己加入其他人的用户聊天。□ 以您的方式社交 浏览或只是快速匹配。使用照片和视频展示您的个性。或者只是滚动、发表评论并点赞您所在地区的新鲜事。□ 发送音乐献词 通过在您发送的消息旁边选择歌曲, 更好地表达您的话语。□ 不允许假货 只有真正对社交感兴趣的人(通过个人资料验证或升级)。此外, 所有照片和视频在显示在个人资料中之前都会经过验证。□ 免费聊天和点赞 Lovemix 上的标准帐户是免费的! 这包括与喜欢您的用户无限发送消息以及每天最多 100 个喜欢。□ 对于每个人 就像爱情一样, 它适合每个人。只要您是一个受过教育、有礼貌的成年人, 想要交朋友、勾搭, 甚至想认识那个特别的人, 我们都欢迎您。□ 有趣的情侣 有些情侣可能会愿意增加第三个人组成三人行, 或者与其他情侣一起摇摆。如果不适合您, 请不要选择您想结识情侣。如果您对应用程序有任何疑问, 请将其发送至 contact@lovemix.com。另请查看 Lovemix 的官方网站: <https://www.lovemix.com> - 订阅价格可能会因您所在的国家/地区而异, 但是您始终可以在应用程序中看到确切的价格 - 除非您在当前订阅期结束前最晚 24 小时取消订阅, 否则您的订阅将自动续订 - 取消订阅后, 您的订阅将保持有效, 直到购买期限结束 - 隐私政策: <https://lovemix.com/privacy> - 条款和条件: <https://lovemix.com/terms>

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患。

© 2025 南明离火 - 移动安全分析平台自动生成