南明离火
移动应用检测平台

ANDROID 静态分析报告

Lovekey • v1.1.0

分析日期: 2024-07-05 14:28:40

应用概览

文件名称:	com.fd.lovekeyboard_1.1.0.apk
文件大小:	32.53MB
应用名称:	Lovekey
软件包名:	com.fd.lovekeyboard
主活动:	com.szcck.lovekey.activity.PrivacyAgreementActivity
版本号:	1.1.0
最小SDK:	24
目标SDK:	34
加固信息:	360加固 加固
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：可能有安全隐患
MD5:	cb70c40420779cc06413ebc82092aaf0
SHA1:	c1664647671143545c5dde884058f1e5b2754ee16
SHA256:	59098cf14b1158733d16bbac1cf145979db679c974ba0be262a4e3ea0b5fb1a4

分析结果严重性分布

高危	中危	信息	安全	关注
4	21	2	1	10

四大组件导出状态统计

Activity组件：47个，其中export的有： 8个
Service组件：3个，其中export的有： 1个
Receiver组件：2个，其中export的有： 1个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

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: CN=Sz, OU=Sz, O=Sz, L=Sz, ST=Sz
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-03 09:29:07+00:00
有效期至: 2111-12-13 09:29:07+00:00
发行人: CN=Sz, OU=Sz, O=Sz, L=Sz, ST=Sz
序列号: 0x1
哈希算法: sha256
证书MD5: e58fada7736610f69a85451044b8195e
证书SHA1: 8b7460eab0729d938eec20566417d23716f23a2d
证书SHA256: e1d4a9154f2ecf88df99d0a45fa97ceec904b28181d2f5c2403e9145ecb25f53
证书SHA512:
2052fbdd6a58a3c6354f10827264236a145427ea2fc521702a7765afd4074f6afae2322ed0a97f8345ae206f70bb762b150b20ad650f3f88c4c90fb750a8b307

公钥算法: rsa
密钥长度: 2048
指纹: bd09d9f93abbb6138e21625a152ed3353b5828bd383f16d40a06de89c747e5d6
找到 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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.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.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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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。
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
com.ss.android.downloadlib.permission.ACCESS_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.fd.lovekeyboard.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

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	应用程序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: **13** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在存在漏洞的已更新 Android 版本上 Android 7.0, [minSdk=24]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	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。
4	Activity设置了TaskAffinity属性 (com.szcck.lovekey.activity.WXPayEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名

5	Activity (com.szcck.lovekey.activity.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
6	Activity-Alias (com.fd.lovekeyboard.wxapi.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
7	Activity-Alias (com.fd.lovekeyboard.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
8	Activity (com.szcck.lovekey.activity.OldMainActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Activity (com.szcck.lovekey.activity.SplashActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
10	Service (com.szcck.lovekey.service.ImeService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_INPUT_METHOD [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.bytedance.ads.convert.BDBridgeActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
12	Activity (com.alipay.sdk.app.PayResultActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Activity (com.alipay.sdk.app.AlipayResultActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **4** | 警告: **6** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	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
2	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
3	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
5	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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	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
8	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
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	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
11	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: MSTG-PLATFORM-7	升级会员：解锁高级权限
12	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
13	已启用远程WebView调试	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	arm64-v8a/libEncryptorP.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
2	arm64-v8a/libGifLib.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

3	arm64-v8a/libglide-webp.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
4	arm64-v8a/libluster.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__strncpy_chk', '__strcpy_chk']	False warning 符号可用

5	arm64-v8a/libpns-2.13.2.1-LogOnlineStandardCuumRelease_alijtca_plus.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
6	arm64-v8a/libterrain.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_PHONE_STATE

本报告由南明离火移动安全分析平台生成

其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.BROADCAST_STICKY

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
www.lovekeyboard.com	安全	否	**IP地址:** 47.236.251.31 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289087 **经度:** 103.850231 **查看:** Google地图
id6.me	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
e.189.cn	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
analytics.oceanengine.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 江苏 **城市:** 徐州 **纬度:** 34.266666 **经度:** 117.166664 **查看:** 高德地图
eco.taobao.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图

msv6.wosms.cn	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
verify.cmpassport.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264570 **查看:** 高德地图
api-e189.21cn.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
opencloud.wostore.cn	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
wap.cmpassport.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 安徽 **城市:** d Islands [Malvinas]FM Micronesia (Federated States of)FO Faroe IslandsFRFr anceGAGabonGB4United Kingdom **纬度:** 31.863815 **经度:** 117.280830 **查看:** 高德地图
nisportal.10010.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
sea.api.lovekeyboard.com	安全	是	**IP地址:** 221.231.92.232 **国家:** 中国 **地区:** 江苏省 **城市:** 南京 **纬度:** 32.0607 **经度:** 118.763 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/ReflectionUtils.java
• https://work.weixin.qq.com/kfid/kfcc7713c5174322e25	com/szcck/lovekey/sdk/WxSdk.java
• https://analytics.oceanengine.com/sdk/app/	com/bytedance/ads/convert/utils/EventReporter.java
• https://eco.taobao.com/router/rest • 2.13.2.1	com/mobile/auth/BuildConfig.java
• 2.13.2.1	com/mobile/auth/gatewayauth/manager/SystemManager.java
• 2.13.2.1	com/mobile/auth/gatewayauth/manager/TokenMaskManager.java
• 2.13.2.1	com/mobile/auth/gatewayauth/manager/VendorSdkInfoManager.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/EncryptUtils.java
• 2.13.2.1 • https://dypnsapi.aliyuncs.com/?	com/mobile/auth/gatewayauth/network/RequestUtil.java
• 2.13.2.1	com/mobile/auth/gatewayauth/LoginAuthActivity.java
• 2.13.2.1	com/mobile/auth/gatewayauth/PhoneNumberAuthHelperProxy.java
• https://wap.cmpassport.com/resources/html/contract.html • https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true • https://e.189.cn/sdk/agreement/detail.do?hidetop=true • https://msv6.wosms.cn/html/oauth/protocol2.html	com/mobile/auth/gatewayauth/Constant.java
• https://sea.api.lovekeyboard.com	com/szcck/lovekey/BuildConfig.java
• 2.13.2.1	com/mobile/auth/gatewayauth/PrivacyDialogActivity.java
• https://dypnsapi.aliyuncs.com/?	com/mobile/auth/gatewayauth/detectnet/e.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/security/CheckProxy.java
• https://nisportal.10010.com:9001/api • https://verify.cmpassport.com/h5/getmobile	com/nirvana/tools/logger/UaidTracker.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/security/CheckHook.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/TokenGenerator.java

• https://www.lovekeyboard.com/agreement/renewal.html • https://www.lovekeyboard.com/agreement/cancel.html • https://www.lovekeyboard.com/agreement/member.html • https://www.lovekeyboard.com/agreement/privacy.html • https://www.lovekeyboard.com/agreement/user.html • https://www.lovekeyboard.com/agreement/phone.html	com/szcck/lovekey/sdk/Constant.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/security/EmulatorDetector.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/security/CheckRoot.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/security/PackageUtils.java
• 2.13.2.1 • https://dypnsapi.aliyuncs.com/?	com/mobile/auth/gatewayauth/network/TopRequestUtils.java
• https://sea.api.lovekeyboard.com	com/szcck/lovekey/api/RetrofitUtil.java
• 2.13.2.1	com/mobile/auth/gatewayauth/utils/AESUtils.java
• https://api-e189.21cn.com/gw/client/accountmsg.do	com/mobile/auth/c/d.java
• https://id6.me/auth/preauth.do	com/mobile/auth/d/a.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
号码认证服务	Alibaba	号码认证服务（Phone Number Verification Service）整合三大运营商特有的网关认证能力，验证用户本机号码与输入号码或账号绑定号码的一致性，升级短信验证码体验，应用于用户注册、登录、安全校验等场景，实现无感知校验。
GlideWebpDecoder	zjupure	GlideWebpDecoder 是一个 Glide 集成库，用于在 Android 平台上解码和显示 webp 图像。它基于 libwebp 项目，并从 Fresco 和 GlideWebpSupport 的一些实现作为参考。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
DataFinder	VolcEngine	基于灵活高效的分析模型，发现用户行为数据的价值，进而转化为促进增长的行动。
移动号码认证	中国移动	号码认证能力提供一键登录、本机号码校验服务。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ，并且轻量和极度灵活。
一键登录和本机号码校验	Alibaba	号码认证服务，整合三大运营商网关认证能力，在用户无感知过程中实现基于手机号码一键完成登录或认证，升级传统短信验证方式，提升用户体验、提高注册转化率、保障业务流程安全； 通信授权服务，提供用户授权数据实时存证、查询和管理能力，授权过程可知可信可追溯，应用于短信、语音等业务场景。

EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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
suzhoufudian@163.com	com/szcck/lovekey/activity/UserCenterActivity.java
suzhoufudian@163.com	com/szcck/lovekey/fragment/home/MineFragment.java
suzhoufudian@163.com	com/szcck/lovekey/adapter/chat/KeyboardTryMsgViewHolder.java

第三方追踪器检测

名称	类别	网址
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

敏感凭证泄露检测

可能的密钥
"authsdk_app_name" : "PhoneNumberAuthSDK"
nsjV57o+ph9iqM0B5aPiMScxWJmCzFRX4WKcj6KGP+3GpzmTyrpavnYQtHasperH
n+APJWeeL+0EjHi0FSf3EmwAtNgcJwLI+u8Lrem+2+qvFY8RRjH3w4jT/wl2HKGEY
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/YHP9utFGOhGk7Xf5L7jOgQz5
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCLShWjAtxJv3g2VPlYOOAv4rnVDdLkdseKm7+KOkCBLV9SKY5oqksFaXcLZ+nRnjnczhze5eGKhevwliUyag6x96GyXl2WaaKoB7Uwl2byl0xB5bNvYzf+x/DKHTSoGJshU6shXWXcjGFq+mUiPhM3WGZoqdY+vvqOWD+tga8XQIDAQAB
014a0668f0IVDUL7/MIGfMA0GCSqGSIb3DQEBAQUAA4G
n4aw0AoExz4atTkUlZJIf9eNLj7ogTlQGANNzE2R/uskFse2GsCqJKFTk4UraBkzf
ngZITTem7Pjdm1V9bJgQ6iQvFHsvT+vNgJ3wAIRd+iCMXm8y96yZhD2+SH5odBYS2

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5se07mkN71qsSJHjZ2Z0+Z+4LlLvf2sz7Md38VAa3EmAOvI7vZp3hbAxicL724ylcmisTPtZQhT/9C+25AELqy9PN9JmzKpwoVTUoJvxG4BoyT49+gGVl6s6zo1byNoHUzTfkmRfmC9MC53HvG8GwKP5xtcdptFjAIcgIR7oAWQIDAQAB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6YCzxZS0FaWDOdtwgcHJ

Google Play 应用市场信息

标题: Lovekey

评分: None **安装:** 50+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.fd.lovekeyboard

开发者信息: Axoso, 8480052415665279098, Hiap Hoe Building. Singapore, 329982, SGP, None, app.ccknetwork@gmail.com,

发布日期: 2024年3月14日 **隐私政策:** Privacy link

关于此应用:

聊天就开始尴尬，回复总说不对话 打开lovekey键盘，轻松帮你回复消息 特色功能 【lovekey键盘】复制对话，点击键盘，一键帮回复 【聊天人设市场】海量聊天人设，轻松提升聊天趣味，打破尴尬 【恋爱开场白】告别I人，无需犹豫，帮你轻松开口say Hi 【聊天亲密度】无论陌生人，还是灵魂伴侣，设置亲密度帮你把握聊天分寸

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。