南明离火
移动应用检测平台

ANDROID 静态分析报告

键盘侠 • v1.0.8

分析日期: 2025-04-09 16:34:09

应用概览

文件名称:	jianpanxia_V1.0.0_2025-04-07_huawei-signed.apk
文件大小:	93.39MB
应用名称:	键盘侠
软件包名:	com.sunteng.newkeyboard
主活动:	com.sunteng.newkeyboard.ui.activity.SettingsActivity
版本号:	1.0.0
最小SDK:	23
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:	46/100 (中风险)
杀软检测:	AI评估：安全
MD5:	931f0564733cac5c3b8ee18c6e3f4f11
SHA1:	15c6cfb3eab8c9a73d7a6073a[illegible]db5e237e
SHA256:	bbd135e3d9337d7a348b1[illegible]edd291e480ecae905083c6e53375ae156e758b0db

分析结果严重性分布

高危	中危	信息	安全	关注
4	12	3	2	2

四大组件导出状态统计

Activity组件：16个，其中export的有： 2个
Service组件：1个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：5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=sun, OU=sunTeng, O=sunTeng, L=GZ, ST=GD, C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-06 08:31:35+00:00
有效期至: 2049-07-31 08:31:35+00:00
发行人: CN=sun, OU=sunTeng, O=sunTeng, L=GZ, ST=GD, C=CN
序列号: 0x1
哈希算法: sha256
证书MD5: 3395219b4539091200ac61e671728efb
证书SHA1: 4d87fdb0490029bfa68fb1e9ed1d1ef22134d1ec
证书SHA256: 4bd5d8b2db230c261c49a11cd5534b405674884ec802b41b38280858e9ff9de8
证书SHA512:
20dc36c3f8292a1a92eb139aed189502c38e061843f8f54cafd53c5fe6143fff042fa6dfc4c1d840e14bfe14a45592348ada57bd1fed988d08f402e4a8f73c00

公钥算法: rsa
密钥长度: 2048
指纹: f9d20ac2b5808457bacbfea432473413bb9af64c36ca892d2313dd169d74ec5f
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.BIND_INPUT_METHOD	签名	绑定到输入法	允许手机用户绑定至输入法的顶级界面。普通应用程序从不需要使用此权限。
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.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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.sunteng.newkeyboard.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

高危: **4** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为绕过证书固定。
4	*	高危	基本配置配置为信任用户安装的证书。
5	*	高危	基本配置配置为绕过证书固定。

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **7** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的、声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	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。
3	Service (com.sunteng.newkeyboard.app.services.CustomKeyBoardService) 受权限保护。 Permission: android.permission.BIND_INPUT_METHOD protectionLevel: signature [android:exported=true]	信息	发现 Service被导出，但受权限保护。
4	Activity设置了TaskAffinity属性 (com.sunteng.newkeyboard.wxapi.WXEntryActivity)	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.sunteng.newkeyboard.wxapi.WXEntryActivity) 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 (com.sunteng.newkeyboard.wxapi.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。

7	Activity设置了TaskAffinity属性 (com.sunteng.newkeyboard.ui.activity.RewardVideoActivity)	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
8	Activity设置了TaskAffinity属性 (com.sunteng.newkeyboard.ui.activity.BuyVipDialogActivity)	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
9	Activity设置了TaskAffinity属性 (com.sunteng.newkeyboard.ui.activity.LoginActivity)	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

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **3** | 安全: **1** | 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
3	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
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	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

6	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
7	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
8	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

应用行为分析

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
00026	方法反射	反射	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
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
00189	获取短信内容	短信	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
00188	获取短信地址	短信	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
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

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
00036	从 res/raw 目录获取资源文件	反射	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	2/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.BIND_INPUT_METHOD android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE 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
kbaipay.clicki.cn	安全	是	**IP地址:** 159.75.176.102 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
appgallery1.huawei.com	安全	是	**IP地址:** 121.36.119.11 **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

URL 链接安全分析

URL信息	源码文件

• http://www.zdic.net/sousuo/?q=%1 • https://www.baidu.com/s?wd=%4 • https://github.com/osfans/trime • http://www.iciba.com/word?w=%3 • http://chewing.csie.net/ • http://android.git.kernel.org/?p=platform/packages/inputmethods/PinyinIME.git • http://www.moedict.tw/ • http://www.xhup.club/?search_word=%4 • https://www.baidu.com/s?wd=%3 • http://www.pkucn.com/viewthread.php?tid=245448 • http://cc-cedict.org/ • https://www.google.com/search?q=%s • https://www.moedict.tw/%3 • http://www.zdic.net/sousuo/?q=%2 • http://www.flypy.com/images/mr.png • http://www.flypy.com • https://hanyu.baidu.com/s?wd=%3	自研引擎-A
• https://kbaipay.clicki.cn/privacy_policy.html	com/sunteng/newkeyboard/ui/fragment/PrivacyPolicyDialog.java
• https://kbaipay.clicki.cn/user/del-count	com/sunteng/newkeyboard/ui/activity/DeleteAccountActivity.java
• https://kbaipay.clicki.cn/privacy_policy.html	com/sunteng/newkeyboard/ui/activity/PrivacyPolicyActivity.java
• https://appgallery1.huawei.com/#/app/C102504217	com/sunteng/newkeyboard/ui/activity/SettingsActivity.java
• https://kbaipay.clicki.cn/user_agreement.html • https://kbaipay.clicki.cn/ai/text-optimization-stream • https://kbaipay.clicki.cn/privacy_policy.html • https://kbaipay.clicki.cn/	com/sunteng/newkeyboard/app/api/NetUrl.java
• https://kbaipay.clicki.cn	o8/m.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
Rime Core	Rime (create by lotem)	Rime 输入法引擎核心库。
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 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
keyboardman@sunteng.com	com/sunteng/newkeyboard/ui/activity/CustomerServiceActivity.java

敏感凭证泄露检测

可能的密钥
aoFlAOtKA7lrb8EaEP6jb5Nmc3eugJku

免责声明及风险提示: