南明离火
移动应用检测平台

ANDROID 静态分析报告

汉王天地 • v1.0.8

分析日期: 2025-03-10 18:48:53

应用概览

文件名称:	com.hanvon.bigmodelproject_1.0.8.apk
文件大小:	51.68MB
应用名称:	汉王天地
软件包名:	com.hanvon.bigmodelproject
主活动:	com.hanvon.bigmodelproject.activity.OneKeyLoginActivity
版本号:	1.0.8
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	e980091e1872c5e64aef04701686b17c
SHA1:	98e129ee51b297e99045093c004f4876d6ce592
SHA256:	b1b1a734a81e60ab82b7953b89276b18f90a4a8be3103008ea5b0a9cedf0f63b

分析结果严重性

高危	警告	信息	安全	关注
3	10	2	1	3

四大组件信息

Activity组件：16个，其中export的有：0个
Service组件：1个，其中export的有：0个
Receiver组件：1个，其中export的有：0个
Provider组件：1个，其中export的有：0个

证书信息

二进制文件已签名

本报告由南明离火移动安全分析平台生成

v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=hanvon
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-18 06:32:29+00:00
有效期至: 2048-09-11 06:32:29+00:00
发行人: CN=hanvon
序列号: 0x359bafa0
哈希算法: sha256
证书MD5: c81babf86e464cb0f2f9b5e9e0e0e752
证书SHA1: 1d3c45f5dd1b9c32f6bd624f15587aa2cad86771
证书SHA256: 3bac20392d96a0f6cea92d0834e1a8fcd67b7f5785aa2fdb44cb7642339bbc16
证书SHA512:
118644bc917a6b8e97b6b360126089d80e76aaeb5ba56679994f7babc184f86344a27b40f844549871dd9e5aa261644bd4cdeb209[illegible]7589d419c7765c994ddee

公钥算法: rsa
密钥长度: 2048
指纹: 19a0b8c15ad957e2476fba6a0876d232fd9f5e9bccbf55106d8d2f61f1048721
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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。
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。

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: **2** | 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	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。

安全漏洞检测

高危: **3** | 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	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	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
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
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	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	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
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	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
10	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
11	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
12	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

行为分析

编号	行为	标签	文件
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
00054	从文件安装其他APK	反射	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
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
00013	读取文件并将其放入流中	文件	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

00191	获取短信收件箱中的消息	短信	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
00033	查询IMEI号	信息收集	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
00012	读取数据并放入缓冲流	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
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
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
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
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
00009	将游标中的数据放入JSON对象	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
00036	从 res/raw 目录获取资源文件	反射	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
00067	查询IMSI号码	信息收集	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	4/30	android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE 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。

域名检测

域名	状态	中国境内	位置信息
5fe2b011624f470db5e54af5682b35f9.oss-cnbj01.cdsgss.com	安全	是	**IP地址:** 210.73.221.116 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397172 **查看:** 高德地图
tiandi.hanvon.com	安全	是	**IP地址:** 220.185.183.50 **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
api.hanvon.com	安全	是	**IP地址:** 220.185.183.50 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://tiandi.hanvon.com/gateway/	com/hanvon/bigmodelproject/AppApplication.java
• https://www.baidu.com/	com/example/xu_mvp_library/base/BaseWebActivity.java
• http://192.168.141.240:7000/audio/audiocount/getfileresult • http://192.168.141.240:7000/audio/audiocount/add	com/hanvon/bigmodelproject/web/constant/ConfigConstants.java
• http://api.hanvon.com/account/api/user/uploadfeedback	com/hanvon/bigmodelproject/activity/question/view/QuestionActivity.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java

• https://5fe2b011624f470db5e54af5682b35f9.oss-cnbj01.cdsgss.com/agreement/gpt/%e6%b1%89%e7%8e%8b%e5%a4%a9%e5%9c%b0%e5%a4%a7%e6%a8%a1%e5%9e%8b%e6%9c%8d%e5%8a%a1%e5%8d%8f%e8%ae%ae.html • http://api.hanvon.com/account/api/ • https://5fe2b011624f470db5e54af5682b35f9.oss-cnbj01.cdsgss.com/agreement/gpt/%e6%b1%89%e7%8e%8b%e5%a4%a9%e5%9c%b0%e5%a4%a7%e6%a8%a1%e5%9e%8b%e9%9a%90%e7%a7%81%e6%94%bf%e7%ad%96.html	com/hanvon/bigmodelproject/util/Constants.java
• wss://tiandi.hanvon.com/websocket	com/hanvon/bigmodelproject/web/algorithm/ClientThread.java
• http://api.hanvon.com/account/api/user/getsoftversion	com/hanvon/bigmodelproject/activity/main/NewMainActivity.java

第三方SDK

SDK名称	开发者	描述信息
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的一款移动应用线上监控平台，为多家知名企业提供服务。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
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 为提供了一种直接，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。

追踪器

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

密钥凭证

可能的密钥
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

06171e8a679eb406e1859a08800955e67cf216d1
65f7f766cac2a664de088544
dAr9DeuZ31JIfisRgqkGz1nEJYXxOS
5fe2b011624f470db5e54af5682b35f9

免责声明及风险提示: