南明离火
移动应用检测平台

ANDROID 静态分析报告

爱心e站 v1.0.0

分析日期: 2025-08-26 16:22:11

应用概览

文件名称:	371240a3c5ee026a172211ba6f505d00-16151082.apk
文件大小:	15.4MB
应用名称:	爱心e站
软件包名:	com.newheyd.JZKFcanjiren
主活动:	com.newheyd.JZKFcanjiren.Activity.SplashActivity
版本号:	1.0.0
最小SDK:	16
目标SDK:	24
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	5/432
杀软检测:	2 个杀毒软件报毒
MD5:	371240a3c5ee026a172211ba6f505d00
SHA1:	43ff63caf85850d7282cd5b58e475de7ac71f0f6
SHA256:	28576f98cb94308f12fcb2c8961286a57d0dec1a9193972f605116846f8fff0

分析结果严重性分布

高危	中危	信息	安全	关注
6	20	2	1	0

四大组件导出状态统计

Activity组件：6个，其中export的有： 3个
Service组件：8个，其中export的有： 2个
Receiver组件：2个，其中export的有： 2个

Provider组件：2个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=shandong, L=jinan, CN=xinzhongtian
签名算法: rsassa_pkcs1v15
有效期自: 2017-02-21 08:10:24+00:00
有效期至: 2042-02-15 08:10:24+00:00
发行人: C=CN, ST=shandong, L=jinan, CN=xinzhongtian
序列号: 0xeaef7a9
哈希算法: sha256
证书MD5: 12c82f4089619ab340a3a7988ffffe1e
证书SHA1: dd51caea4f760a6e805b45e6390f5562e1c12b44
证书SHA256: 9a740abd170cd975ded8b0e2d44cb5494e152fb49e0c120015ad393750b082d3
证书SHA512:
ebffa61d553bb87dfd9b956312854fe240daf5a509c50eecffa09ac2f9904e4823848694f41e7060fde69eac551d54cc2489416848d...54b6ff7ce32b50dc0499

公钥算法: rsa
密钥长度: 2048
指纹: 1033381270545dce4f05349eabe28bf72bd1289ea366ca695d3d9138912b374...
共检测到 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.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_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。
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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。

android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	Schemes: tencent100424468://,

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **4** | 警告: **10** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	Activity (com.tencent.tauth.AuthActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity（com.tencent.tauth.AuthActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（24） 升级至 28 及以上以获得平台级防护。
4	Activity (com.tencent.tauth.AuthActivity) 未受保护。存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
5	Activity (com.newheyd.JZKFcanjiren.wxapi.WXEntryActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（24）升级至 29 及以上，从平台层面修复该漏洞。
6	Activity (com.newheyd.JZKFcanjiren.wxapi.WXEntryActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Broadcast Receiver (com.newheyd.JZKFcanjiren.Utils.VesionUpdate.receivers.ApkInstallReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
8	Service (com.igexin.sdk.PushService) 未受保护。[android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
9	Broadcast Receiver (com.igexin.sdk.PushReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
10	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.PushActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
11	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.GActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。

12	Activity (com.igexin.sdk.GActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（24）升级至 29 及以上，从平台层面修复该漏洞。
13	Activity (com.igexin.sdk.GActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Service (com.newheyd.JZKFcanjiren.service.GeTuiPushService) 未受保护。[android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **1** | 警告: **9** | 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	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
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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄露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

5	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
6	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
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	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
9	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
10	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
11	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

12	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
13	此应用程序使用SQL Cipher。SQL Cipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00034	查询当前数据网络类型	信息收集 网络	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
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
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
00054	从文件安装其他APK	反射	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
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
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
00035	查询已安装的包列表	反射	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
00091	从广播中检索数据	信息收集	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
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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限

00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
00031	检查当前正在运行的应用程序列表	反射 信息收集	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
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
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
00033	查询IMEI号	信息收集	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
00013	读取文件并将其放入流中	文件	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	14/30	android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.CAMERA android.permission.CALL_PHONE android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.READ_CONTACTS android.permission.WRITE_SETTINGS android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	6/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE

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
iws.openspeech.cn	安全	是	**IP**地址: 36.7.109.160 国家: 中国 地区: 中国安徽 城市: 合肥 纬度: 31.820592 经度: 117.227219 查看: 高德地图
data.openspeech.cn	安全	是	**IP**地址: 117.48.148.47 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图
www.service.sddpf.org.cn	安全	否	No Geolocation information available.
scs.openspeech.cn	安全	是	**IP**地址: 117.48.148.47 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.microsoft.com/typography/fonts/default.aspx • http://www.microsoft.com/typography/ctfontshttp	自研引擎-A
• http://data.openspeech.cn/index.php/clientrequest/clientcollect/iscollect	com/iflytek/sunflower/task/a.java
• http://www.service.sddpf.org.cn/sdclizki	com/newheyd/JZKFcanjiren/config/NewHYConfig.java
• http://iws.openspeech.cn/online_param/config_update.php • http://scs.openspeech.cn/scs	com/iflytek/sunflower/config/a.java
• 10.0.0.200	com/tencent/mid/a/b.java
• http://119.164.253.214:6888/jncl/m/life/appweblifeinfo/lifeview • http://192.168.47.105:8080/jzfw/m/dynamicupdate/basic/gdeformitybasicinfo/findlist	com/newheyd/JZKFcanjiren/net/RequestServiceList.java
• http://pcsv1.map.bdimg.com/scape/?qt=pdata&sid=	com/baidu/panosdk/plugin/indoor/view/IndoorAlbumView.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。 您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
讯飞 SDK	科大讯飞	讯飞开放平台作为全球首个开放的智能交互技术服务平台，致力于为开发者打造一站式智能人机交互解决方案。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
U-Share 社会化分享	Umeng	帮助应用或游戏快速具备国内外多平台分享、第三方登录功能，SDK 包小，集成成本低，平台覆盖全。
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。
Tinker	Tencent	Tinker 是适用于 Android 的热更新程序库，它支持无需重新安装 apk 来更新 dex，库和资源。

邮箱地址敏感信息提取

EMAIL	源码文件
ctwap@mycdma.cn	com/tencent/mid/a/b.java

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计=> "UMENG_CHANNEL" : "yingyongbao"
友盟统计的=> "UMENG_APPKEY" : "5b30a2a7a40fa3095a000029"

个推-推送服务的=> "PUSH_APPKEY" : "9LneMYzVNl7aKYhOMPRpJ3"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "wLQmGtMfsSmmqCUUqLDZXKRDgplAnQ3d"
个推-推送服务的=> "PUSH_APPSECRET" : "SAcypEkJAW6jQRY31eJ2J8"
个推-推送服务的=> "PUSH_APPID" : "O6pD0c6lAW5vM6hhihn544"
4kU71lN96TJUomD1vOU9lgj9U+kKmxDPLVM+zzjst5U=
6X8Y4XdM2Vhvn0KfzcEatGnWaNU=
d4624c36b6795d1d99dcf0547af5443d
03a976511e2cbe3a7f26808fb7af3c05

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。