南明离火
移动应用检测平台

ANDROID 静态分析报告

Hyouka private • v5.8.9

分析日期: 2025-08-28 22:43:21

应用概览

文件名称:	Hyouka private v5.8.9.apk
文件大小:	44.86MB
应用名称:	Hyouka private
软件包名:	com.beint.zangi
主活动:	com.beint.project.NavigationManagerActivity
版本号:	5.8.9
最小SDK:	21
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:	55/100 (中风险)
跟踪器检测:	4/432
杀软检测:	2 个杀毒软件报毒
MD5:	97cbbe92937aeb61bbe679984179ecf4
SHA1:	bc5d9d24def11a[illegible]d6d151f26ec09999dca209
SHA256:	1142bd4c1fc7c7c766d745cf31a1a6aabad6c89bacce2f7e0bd63f8df7f8a40f

分析结果严重性分布

高危	中危	信息	安全	关注
0	38	3	3	0

四大组件导出状态统计

Activity组件：[illegible]个，其中export的有： 12个
Service组件：17个，其中export的有： 7个
Receiver组件：11个，其中export的有： 7个

Provider组件：4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: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640[illegible]053abfea3039772720[illegible]9[illegible]704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e[illegible]
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.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.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.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
android.permission.READ_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
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。
com.beint.zangi.permission.MAPS_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
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.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.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。
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.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。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.RAISED_THREAD_PRIORITY	未知	未知权限	来自 android 引用的未知权限。
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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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。
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
com.adobe.reader.misc.ARFileProvider.READ_CONTENT	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.ARFileProvider.WRITE_CONTENT	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.READ_CONTENT	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.WRITE_CONTENT	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.ARFileProvider.READ_DATABASE	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.ARFileProvider.WRITE_DATABASE	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.ARFileProvider	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.READ_DATABASE	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader.misc.WRITE_DATABASE	未知	未知权限	来自 android 引用的未知权限。
com.adobe.reader	未知	未知权限	来自 android 引用的未知权限。
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.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.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
com.google.android.c2dm.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.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
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。

com.beint.zangi.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.beint.project.NativeContactsHandlerActivity	Schemes: https://, Hosts: zangi.com, services.zangi.com, Mime Types: vnd.android.cursor.item/vnd.com.zangi.chat, vnd.android.cursor.item/vnd.com.zangi.audio, vnd.android.cursor.item/vnd.com.zangi.video, vnd.android.cursor.item/vnd.com.zangi.out, Path Prefixes: /dl/,
com.beint.project.MainActivity	Schemes: https://, zangi://, Hosts: zangi.com, resolve, services, networks, Path Prefixes: /services/, /networks/,
com.beint.project.screens.CallActivity	Schemes: tel://,

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: **0** | 警告: **28** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Service (com.beint.project.services.call_service_foreground.ForegroundService) 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。
3	Service (com.beint.project.core.FileWorker.FileDownloadUploadService) 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。
4	Broadcast Receiver (com.beint.project.screens.P2PConnection.BroadcastForWiFi) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
5	Broadcast Receiver (com.beint.project.ReplyMessageBroadcastReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (com.beint.project.CallActionReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.beint.project.NativeContactsHandleActivity) 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。
8	Activity (com.beint.project.MainActivity) 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。
9	Activity (com.beint.project.screens.BaseFragmentActivitySingle) 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。
10	Activity (com.beint.project.screens.ShareActivity) 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。

11	Activity (com.beint.project.screens.CallActivity) 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。
12	Activity (com.beint.project.screens.ProfileImageActivity) 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。
13	Activity (com.beint.project.screens.HomeActivity) 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	Activity (com.beint.project.screens.EmptyActivity) 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。
15	Activity (com.beint.project.screens.CallingFragmentActivity) 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。
16	Broadcast Receiver (com.beint.project.HeadphoneReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
17	Broadcast Receiver (com.beint.project.MediaButtonIntentReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
18	Broadcast Receiver (com.beint.project.NetworkChangeReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
19	Service (com.beint.project.push.FireBaseListener) 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。
20	Service (com.beint.project.utils.ContactsSyncAdapterService) 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。
21	Service (com.beint.project.utils.AuthenticatorService) 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。

22	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
23	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
24	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
25	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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。
26	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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。
27	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。
28	高优先级 Intent（1000000） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **0** | 警告: **8** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	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
2	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
3	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
4	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
5	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
6	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
7	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	警告	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
8	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

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	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
11	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
12	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	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/libprojectcore.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	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: ['__strchr_chk', '__memmove_chk', '__strncpy_chk', '__FD_SET_chk', '__strrchr_chk', '__memset_chk', '__strlen_chk', '__strcpy_chk', '__vsprintf_chk', '__vsnprintf_chk', '__strcat_chk', '__memcpy_chk']	True info 符号被剥离

应用行为分析

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
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
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	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
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
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
00189	获取短信内容	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
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
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
00024	Base64解码后写入文件	反射 文件	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
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
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
00036	从 res/raw 目录获取资源文件	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
00028	从assets目录中读取文件	文件	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
00092	发送广播	命令	升级会员：解锁高级权限
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	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
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
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 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

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
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
00126	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
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
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
00006	安排录制任务	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
00121	创建目录	文件 命令	升级会员：解锁高级权限
00015	将缓冲流（数据）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
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
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
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
00153	通过 HTTP 发送二进制数据	http	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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	13/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WAKE_LOCK android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.CALL_PHONE android.permission.GET_ACCOUNTS android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	20/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.BROADCAST_STICKY android.permission.ACCESS_NOTIFICATION_POLICY android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.READ_EXTERNAL_STORAGE android.permission.AUTHENTICATE_ACCOUNTS com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.REORDER_TASKS android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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.smpte-ra.org	安全	否	**IP地址:** 151.101.193.91 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
stripe.com	安全	否	**IP地址:** 35.167.54.49 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.67[illegible] **查看:** Google 地图
api.giphy.com	安全	否	**IP地址:** 151.101.193.91 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
zangi.com	安全	否	**IP地址:** 35.167.54.49 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
maps.apple.com	安全	是	**IP地址:** 58.220.70.19 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
relaxng.org	安全	否	**IP地址:** 185.199.110.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

etherx.jabber.org	安全	否	**IP地址:** 208.68.163.210 国家: 美国 地区: 爱荷华州 城市: 蒙蒂塞洛 纬度: 42.238338 经度: -91.187088 查看: Google 地图
e.crashlytics.com	安全	否	No Geolocation information available.
test-api.zangi.io	安全	否	No Geolocation information available.
zconfiguration.s3.eu-west-1.amazonaws.com	安全	否	**IP地址:** 3.5.66.95 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图
www.vr-messaging.com	安全	否	No Geolocation information available.
www.oasis-open.org	安全	否	**IP地址:** 52.214.4.202 国家: 美国 地区: 得克萨斯州 城市: 圣安东尼奥 纬度: 29.424120 经度: -98.493729 查看: Google 地图
api-7945875896688690698-914144.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 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.zangi.com	安全	否	**IP地址:** 34.244.97.69 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图
services.zangi.com	安全	否	**IP地址:** 52.214.4.202 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图

api.stripe.com	安全	否	**IP地址:** 52.214.4.202 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
settings.crashlytics.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://fsf.org • http://www.teluu.com • http://www.cryptopp.com • http://www-ccrma.stanford.edu • http://www.ilbcfreeware.org/documentation/gips_iLBClicense.pdf	自研引擎-A
• https://www.vr-messaging.com/privacy_policy.php	com/beint/project/screens/ui/RegistrationPermissionFragmentUI.java
• 224.0.0.251	ya/i.java
• https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	va/q.java
• https://e.crashlytics.com/spi/v2/events	va/k.java
• https://%s/%s/%s	s7/c.java
• http://maps.apple.com/maps?q=	com/beint/project/utils/ShareManger.java
• 4.7.2.2	com/beint/project/core/managers/SystemServiceManager.java
• https://www.vr-messaging.com/privacy_policy.php	com/beint/project/screens/register/RegistrationPermissionsFragment.java
• http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
• http://testapi.zangi.io/v3/auth/check/zz	com/beint/project/core/services/impl/ZangiHTTPServices.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	w6/s.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	d7/f.java
• http://play.google.com/store/apps/details?id=	com/beint/project/screens/RateZangiApp.java
• 4.7.2.2	com/beint/project/utils/EsyLoader.java

• https://play.google.com/store/apps/details?id=com.beint.zangi	com/beint/project/screens/P2PConnection/DataTransferFragment.java
• https://graph.facebook.com/	com/beint/project/core/services/impl/ZangiProfileServiceImpl.java
• https://stripe.com/docs/stripe.js	y9/h.java
• https://api.giphy.com	g3/b.java
• http://test-api.zangi.io/v3/auth/check/{prefix}	com/beint/project/core/services/impl/HTTPServicesApi.java
• https://api.stripe.com	aa/e.java
• 127.0.0.1 • 37.48.99.22 • 192.168.0.135 • 188.138.101.132 • 85.25.119.154 • 37.48.99.23 • 37.48.99.1 • 37.48.99.2 • 85.25.153.12	com/beint/project/screens/settings/more/settings/ServerFragment.java
• http://play.google.com/store/apps/details?id=	com/beint/project/screens/settings/free/minutes/RateGetFragment.java
• https://zangi.com/features/security • http://www.zangi.com • https://api-794587589668869O698-914144.firebaseio.com • https://services.zangi.com/ • https://zangi.com/terms-of-use • https://zangi.com/networks • http://www.zangi.com/contact • https://zangi.com/privacy-policy	自研引擎-S
• file:///etc/xml/catalog • 52.215.160.30 • http://zangi.com/i/ • http://relaxng.org/ns/structure/1.0 • http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd • http://zangi.com • 192.168.0.232 • https://zconfiguration.s3.eu-west-1.amazonaws.com/hosts.txt • 192.168.0.209 • 85.25.137.50 • https://v4-services • 192.168.43.153 • http://zangi.com/top-up • 169.254.100.187 • http://etherx.jabber.org/streams	lib/arm64-v8a/libprojectcore.so

Firebase 配置安全检测

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://api-7945875896688690698-914144.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/293922712990/namespaces/firebase:fetch?key=AIzaSyBuRFyzlqhgZ9qDe9g2vNmB575yda8VCgI ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现了各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
Jetpack Test	Google	在 Android 中进行测试。
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 Sign-In	Google	提供使用 Google 登录的 API。
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。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
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 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
support@stripe.com	aa/e.java
support@zangi.com	lib/arm64-v8a/libprojectcore.so

第三方追踪器检测

名称	类别	网址
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "@7F1202F5"
凭证信息=> "io.fabric.ApiKey" : "68d8d04c48350cedad5a3c0249c6dcee854d39a8"
"private_chat_notifications" : "Chats"
"app_id" : "463889927035400"
"password" : "Senha"
"firebase_database_url" : "https://ap[illegible]1587589668869069[illegible]firebaseio.com"
"private_chat_notifications" : "Bate-papo"
"google_crash_reporting_api_key" : "AIzaSyBuRF[illegible]qhgZ9qDe9g2vNmB575yda8VCgI"
"com.google.firebase.crashlytics.mapping_file_id" : "f2317961b554472b933fb6c0497012e3"
"map_key" : "AIzaSyCNN0O1h-N[illegible]GFOLOmkvNqI6n1F0"
"google_app_id" : "1:293922[illegible]:android:ec0fc6a0a55fde0c"
"password" : "Password"
"google_api_key" : "AIzaSyBuRFyzlqhgZ9qDe9g2vNmB575yda8VCgI"
2M+Wrf[illegible]d5izmp4Q0yxmRXZiCYXYC+dAU1jI
9A04F079-9840-4286-AB92-E65BE0885F95

470fa2b4ae81cd56ecbcda9735803434cec591fa
e1OuEE3WqOrsVzWKyeh2FcbYXEMcNmag

Google Play 应用市场信息

标题: 赞吉信使

评分: 4.3918257 **安装:** 10,000,000+ **价格:** 0 **Android版本支持:** **分类:** 通讯 **Play Store URL:** com.beint.zangi

开发者信息: Secret Phone, Inc, Secret+Phone,+Inc, None, https://zangi.com, support@zangi.com,

发布日期: 2014年11月18日 **隐私政策:** Privacy link

关于此应用:

通过您的 livecom 运营商和全包解决方案 Zangi 进行免费的高清品质语音和视频通话，以及免费聊天。如果您正在寻找一款可以方便地从单一源实现所有通讯需求且具备最佳可用质量的应用程序，则无需进一步寻找了，Zangi 就是您所要的。 使 用 Zangi 的 Android “原生”拨号器或者从您的联系人列表中选择一个名字，进行 Zangi 网内免费通话，或者呼叫GSM 网络或座机进行低费用通话（以及发送短信），在对方无互联网连接时也不会中断您的呼叫。如果您的互联网连接速度很慢，您仍可通过我们的回拨服务使用 Zangi 拨打电话：让我们为您建立连接，以便您随时随地与任何人保持联系。 您的主要手机号码是您注册 Zangi 的身份代码，也是您的 Zangi 号码，方便其他人呼叫。有了 Zangi，您就拥有了期望从 GSM 电话服务获得的所有功能，以及新型网络电话的所有功能，如免费语音、视频和聊天，及其更方便的融合，并提供更好的质量。我们还率先推出了一项可在旅途中为您提供支持的独特免费漫游服务：您的朋友和家人无需知道您在其他地方的号码，他们只需拨打您的 Zangi 号码即可联系到您。 有了 Zangi，您可以以最佳方式使用电池和手机资源：视频和音频通话再也不会在几分钟内耗尽您的电池。Zangi 会让人忘记充电器。实现免费通话，同时具备高清品质和最低的上网速度。

免责声明及风险提示: