南明离火
移动应用检测平台

ANDROID 静态分析报告

云上营家 • v1.0.2

分析日期: 2024-07-07 10:21:58

应用概览

文件名称:	com.inja.portal.pro_1.0.2.apk
文件大小:	26.12MB
应用名称:	云上营家
软件包名:	com.inja.portal.pro
主活动:	com.hand.hippius.activity.SplashActivity
版本号:	1.0.2
最小SDK:	21
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	4/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	9ba2fd16f6ed45b0dd8309bc909fede6
SHA1:	4a135c2fd39ec02d6e00a723[illegible]c04ca04cec
SHA256:	dd97619b5ef1b8884de6[illegible]8a57903e6fa37b[illegible]082f9dd2f4b647a9f

分析结果严重性分布

高危	中危	信息	安全	关注
2	45	3	1	12

四大组件导出状态统计

Activity组件：119个，其中export的有： 19个
Service组件：22个，其中export的有： 7个
Receiver组件：12个，其中export的有： 6个
Provider组件：4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: False
v4 签名: False
主题: CN=Hand
签名算法: rsassa_pkcs1v15
有效期自: 2020-05-20 06:11:39+00:00
有效期至: 2045-05-14 06:11:39+00:00
发行人: CN=Hand
序列号: 0x38c3441d
哈希算法: sha256
证书MD5: 2fa97b8e7a84361c279380b61f8a3a9f
证书SHA1: cac803629300a8933f5a2c8f25e5dff27e91ada0
证书SHA256: f9140dcb47b0886c2a086e6feb3246a17649fdc8982261b269a25343dd3ee6c5
证书SHA512:
4e29f837d51183f809369f7d8a3ee83020da3b28c9b3ca5ba12f071753b67705fe2789c92d61c3603405685187ca42f5cad37058a1a2feeefc6039596bfb88a

公钥算法: rsa
密钥长度: 2048
指纹: 4b29f24c237efa24caff79defdb16bbd3f1cc65103fe1e244a7ff43e7221505a
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.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.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.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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
com.android.browser.permission.READ_HISTORY_BOOKMARKS	危险	获取自带浏览器上网记录	恶意代码可有利用此权限窃取用户的上网记录和书签。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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错略的经纬度信息，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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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.RECORD_VIDEO	未知	未知权限	来自 android 引用的未知权限。
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.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.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用，应用程序应改为请求USE_BIOMETRIC
com.inja.portal.pro.permission.JOPERATE_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.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。
com.inja.portal.pro.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。
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.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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。

com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
com.inja.portal.pro.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	未知权限	来自 android 引用的未知权限。
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

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.hand.hippius.activity.SplashActivity	Schemes: hippius://,
com.hand.hippius.activity.icon5	Schemes: hippius://,
com.hand.hippius.activity.icon4	Schemes: hippius://,
com.hand.hippius.activity.icon3	Schemes: hippius://,
com.hand.hippius.activity.icon2	Schemes: hippius://,
com.hand.hippius.activity.icon1	Schemes: hippius://,
com.hand.mainlibrary.activity.HomeActivity	Schemes: inja://, Hosts: app, Paths: /logout,
com.tencent.tauth.AuthActivity	Schemes: tencent101848397://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 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。

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: **34** | 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有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	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。
3	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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-Alias (com.hand.hippius.activity.icon5) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
5	Activity-Alias (com.hand.hippius.activity.icon4) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
6	Activity-Alias (com.hand.hippius.activity.icon3) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
7	Activity-Alias (com.hand.hippius.activity.icon2) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
8	Activity-Alias (com.hand.hippius.activity.icon1) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
9	Activity (com.hand.mainlibrary.activity.HomeActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
10	Activity (com.hand.im.activity.ConversationActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
11	Activity (com.google.zxing.client.android.encode.EncodeActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

12	Activity (com.google.zxing.client.android.book.SearchBookContentsActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
13	Activity (com.google.zxing.client.android.share.ShareActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
14	Service (com.jpush.PushService) 未被保护。 [android:exported=true]	警告	发现 Service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。
15	Service (com.jpush.JPUSHMessageReceiver) 未被保护。 [android:exported=true]	警告	发现 Service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。
16	Activity (com.inja.portal.pro.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。
17	Activity (com.inja.portal.pro.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。
18	Activity (com.tencent.tauth.AuthActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
19	Activity (com.sina.weibo.sdk.share.WbShareTransActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
20	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
21	Service (com.google.firebase.iid.FirebaseInstanceIdService) 未被保护。 [android:exported=true]	警告	发现 Service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。
22	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。

本报告由南明离火移动安全分析平台生成

23	Activity (cn.jpush.android.ui.PopWinActivity) 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。
24	Activity (cn.jpush.android.ui.PushActivity) 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。
25	Activity (cn.jpush.android.service.JNotifyActivity) 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。
26	Activity (cn.android.service.JTransitActivity) 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。
27	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 未被保护。[android:exported=true]	警告	发现 Service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。
28	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver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。
29	Broadcast Receiver (cn.jpush.android.service.PluginXiaomiPlatformsReceiver) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver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。
30	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。
31	Broadcast Receiver (cn.jpush.android.service.PluginMeizuPlatformsReceiver) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver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。
32	Service (cn.jpush.android.service.PluginOppoPushService) 受权限保护, 但是应该检查权限的保护级别。Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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。
33	Service (com.heytap.msp.push.service.DataMessageCallbackService) 受权限保护, 但是应该检查权限的保护级别。Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [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。

34	Broadcast Receiver (cn.jpush.android.service.PluginVivoMessageReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
35	Service (com.vivo.push.sdk.service.CommandClientService) 未被保护。 [android:exported=true]	警告	发现 Service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。
36	高优先级的Intent (1000) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **1** | 警告: **9** | 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
2	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
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
5	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
6	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

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	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
9	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
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	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
12	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
13	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
14	此应用程序使用SQL Cipher。SQLCipher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

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)	SYMBOLSSTRIPPED(裁剪符号表)
1	arm64-v8a/libzbarjni.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

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	13/30	android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.GET_ACCOUNTS android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.GET_TASKS
其它常用权限	12/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION 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
gateway.inja.com	安全	是	**IP地址:** 203.107.44.30 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
newportal-it.vsvec.com	安全	是	**IP地址:** 8.129.0.154 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
yongyou-c7ca5f-3498.udesk.cn	安全	是	**IP地址:** 203.107.44.30 **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

data.openspeech.cn	安全	是	**IP地址:** 203.107.44.30 **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
greenrobot.org	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
bi.inja.com	安全	是	**IP地址:** 10.41.41.207 **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
yunnan.12388.gov.cn	安全	是	**IP地址:** 203.107.44.30 **国家:** 中国 **地区:** 云南 **城市:** 昆明 **纬度:** 25.038891 **经度:** 102.718330 **查看:** 高德地图
aip.baidubce.com	安全	是	**IP地址:** 203.107.44.30 **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
gatewayapp.inja.com	安全	是	**IP地址:** 47.112.244.225 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
iws.openspeech.cn	安全	是	**IP地址:** 203.107.44.30 **国家:** 中国 **地区:** 安徽 **城市:** 合肥 **纬度:** 31.863815 **经度:** 117.280830 **查看:** 高德地图

scs.openspeech.cn	安全	是	**IP地址:** 203.107.44.30 **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
www.pgyer.com	安全	是	**IP地址:** 203.107.44.30 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161580 **查看:** 高德地图
paygate-yf.meituan.com	安全	是	**IP地址:** 103.37.152.89 **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
• https://github.com/videojs/video.js/issues/2617 • https://zxing.appspot.com/generator • http://underscorejs.org/LICENSE • https://git.io/vMpjB • http://photoswipe.com • https://tools.ietf.org/html/draft-pantos-http-live-streaming-23 • https://bit.ly/2ZqJzkp • https://www.inja.com/product/bidNoticeDetails.html?headerId= • https://vjs.zencdn.net/vttjs/0.14.1/vtt.min.js • https://lodash.com/ • https://openjsf.org/ • https://zxing.appspot.com/generator • https://www.inja.com/product/winBidDetails.html?headerId • https://twitter.com/intent/tweet?text= • https://lodash.com/license • https://www.facebook.com/sharer/sharer.php?u= • http://www.pinterest.com/pin/create/button/?url= • http://feross.org • https://gateway.inja.com • https://sms.inja.com/images/index/logo.png	自研引擎-A
• https://gatewayapp.inja.com	com/hand/messages/fragment/CollectionFragment.java
• https://gatewayapp.inja.com/	com/hand/im/activity/MsgFileSearchActivity.java
• http://newportalsit.ysyec.com/index/privacypolicy.html • https://gateway.inja.com • https://gatewayapp.inja.com/	com/hand/baselibrary/BuildConfig.java

• http://newportalsit.ysyec.com/index/privacypolicy.html	com/hand/baselibrary/activity/ProtocolActivity.java
• https://gatewayapp.inja.com/	com/hand/im/activity/MsgRecordActivity.java
• https://gatewayapp.inja.com/	com/hand/im/activity/MultiMsgActivity.java
• http://scs.openspeech.cn/scs • http://iws.openspeech.cn/online_param/config_update.php	com/iflytek/sunflower/config/a.java
• https://aip.baidubce.com/rest/2.0/ocr/v1/business_card • https://aip.baidubce.com/oauth/2.0/token?grant_type=client_credentials	com/hand/businesscard/ApiPresenter.java
• https://gatewayapp.inja.com/hipspfm/hippius/v1/users/public/captcha/	com/hand/baselibrary/widget/imagecode/ImageCodeResetPresenter.java
• https://gatewayapp.inja.com/oauth/public/captcha/	com/hand/baselibrary/widget/imagecode/ImageDialogPresenter.java
• https://gateway.inja.com • https://gatewayapp.inja.com/	com/hand/baselibrary/config/Constants.java
• https://gatewayapp.inja.com/	com/hand/im/HandIM.java
• http://data.openspeech.cn/index.php/clientrequest/clientcollect/iscollect	com/iflytek/sunflower/task/a.java
• https://gatewayapp.inja.com/	com/hand/baselibrary/service/AppDownloadService.java
• https://gatewayapp.inja.com/	com/hand/yndt/applications/fragment/ApplicationFragment.java
• https://gatewayapp.inja.com/	com/hand/im/widget/MsgResendDialog.java
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
• http://bi.inja.com/webroot/decision/ssologin?token=%1$s&redirect=http://bi.inja.com/webroot/decision • https://gatewayapp.inja.com/	com/hand/yndt/contacts/fragment/MineFragment.java
• https://paygate.vf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/a.java
• https://gatewayapp.inja.com/	com/hand/yndt/applications/glide/AppUtil.java
• https://gatewayapp.inja.com/	com/hand/mainlibrary/service/SplashDownloadService.java
• https://gatewayapp.inja.com/	com/hand/mainlibrary/activity/HomeActivity.java
• https://www.pgyer.com/yjysios • https://gatewayapp.inja.com/	com/hand/plugin/BaseBridge.java

• https://yongyou-c7ca5f-8498.udesk.cn/im_client/?web_plugin_id=124411&cur_title=&src_url=&cur_url=http%3a%2f%2fportalsit.ysyec.com%2fportal&pre_url=http%3a%2f%2fportalsit.ysyec.com%2fportal&_invite_user_key=9b5eeca4-ff35-4186-80af-b00bfc531461 • https://yunnan.12388.gov.cn/	com/hand/messages/fragment/MessageFragment.java
• https://gatewayapp.inja.com/	com/hand/baselibrary/utils/ImageLoadUtils.java
• https://gatewayapp.inja.com/	com/hand/baselibrary/net/download/RetrofitDownload2Client.java
• https://gateway.inja.com • https://gatewayapp.inja.com/	com/hand/baselibrary/net/RetrofitClient.java
• https://gatewayapp.inja.com/	com/hand/baselibrary/net/download/RetrofitDownloadClient.java
• https://gatewayapp.inja.com/	com/hand/baselibrary/net/RetrofitUploadClient.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
iconv	GNU	iconv 是一个计算机程序以及一套应用程序编程接口的名称，它的作用是在多种国际编码格式之间进行文本内码的转换。
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。
360 加固	360	360 加固保是基于 360 核心加密技术，对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。
ZBar	spadix	ZBar 是一个用于从各种来源读取条码的开源软件套件, 它支持许多流行的条码类型, 包括 EAN-13/UPC-A, UPC-E, EAN-8, Code 128, Code 39, 交叉 2/5 码(Interleaved 2 of 5)和二维码(QR Code)
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。 开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。 JPush 全面支持 Android, iOS, Winphone 三大手机平台。
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。
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。
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。
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。
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。

MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
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。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
service@inja.com	com/hand/messages/fragment/MessageFragment.java

第三方追踪器检测

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

敏感凭证泄露检测

可能的密钥
vivo推送的=> "local_iv" : "MzMsMzQsMzIsMzYsMzcsMzgsMiksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwiQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDM2LDM1LDM0LDMzLDMyLDM3LDM4LDM5LDQwLDQxLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzIsMzIsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI="
OPPO推送的=> "OPPO_APPKEY" : "OP-oppo的APPKEY"
OPPO推送的=> "OPPO_APPSECRET" : "OP-oppo的APPSECRET"
荣耀推送的=> "com.hihonor.push.app_id" : "honor的APPID"
小米推送的=> "XIAOMI_APPID" : "MI-小米的APPID"
极光推送的=> "JPUSH_CHANNEL" : "inja_dev"
vivo推送的=> "com.vivo.push.app_id" : "vivo的APPID"
魅族推送的=> "MEIZU_APPKEY" : "MZ-魅族的APPKEY"
魅族推送的=> "MEIZU_APPID" : "MZ-魅族的APPID"

本报告由南明离火移动安全分析平台生成

极光推送的=> "JPUSH_APPKEY" : "700cba0f60b18a7148a63d22"
小米推送的=> "XIAOMI_APPKEY" : "MI-小米的APPKEY"
OPPO推送的=> "OPPO_APPID" : "OP-oppo的APPID"
vivo推送的=> "com.vivo.push.api_key" : "vivo的APPKEY"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "cc4wVL1DrGzROARd3j1OleZYipo6b3jP"
"base_password" : "Password"
"base_search_key" : "Search"
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJL0JkqsUoK6kt3JyogsgqNp9VDGDp+t3ZAGMbVoMPdHNT2nfiIVh9ZMNHF7g2XiAa8O8AQWyh2PjMR0NiUSVQMCAwEAAQ==
700cba0f60b18a7148a63d22
39280363481451541647
2FsPONw4QOqEQkzYvoiuVATWxbyQmsCJ
5a0a6f10f29d985d00000204
9b5eeca4-ff35-4186-80af-b00bfc531461
7b494b48d739e8f0db98f1fbe080c254
2FDgvkGVlKtvyo6NX8HbSycCiDHWR2gaqJRI3JrAqT9lGxZAxTnmUE4MNnhHWfoNZJHX2
d09bf5c069b761f038d48e8b
-39280363481451541647

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与安全评估框架。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。