南明离火
移动应用检测平台

ANDROID 静态分析报告

教育考试指挥 • v3.0.0.066

分析日期: 2024-06-13 17:20:51

应用概览

文件名称:	neeaEM_V3.0.0.066_Release_Build66.apk
文件大小:	46.81MB
应用名称:	教育考试指挥
软件包名:	com.jf.gk.client
主活动:	com.jf.gk.client.StartActivity
版本号:	3.0.0.066
最小SDK:	21
目标SDK:	26
加固信息:	360加固 加固
应用程序安全分数:	34/100 (高风险)
跟踪器检测:	3/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	4c7ee0bdbbe9f0f2a84dede994d0cba8
SHA1:	40c114336dda17db1840ac8c47c2f4ffbe4d2ad4
SHA256:	de8f04b723db0ef3170f0b0bb2df2f0bda7cb971fa6afb068f477f20142a4d40

分析结果严重性分布

高危	中危	信息	安全	关注
15	29	2	1	3

四大组件导出状态统计

Activity组件：67个，其中export的有： 3个
Service组件：18个，其中export的有： 9个
Receiver组件：13个，其中export的有： 3个
Provider组件：12个，其中export的有： 1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: C=zh, ST=sichuang, L=chengdu, O=hw, OU=hw, CN=homework
签名算法: rsassa_pkcs1v15
有效期自: 2017-04-14 03:28:55+00:00
有效期至: 2042-04-08 03:28:55+00:00
发行人: C=zh, ST=sichuang, L=chengdu, O=hw, OU=hw, CN=homework
序列号: 0x3c25ca59
哈希算法: sha256
证书MD5: 8896cd96b7bdcb600e5f0ce0ec47001e
证书SHA1: 26a54c4e3649c78a163ac7136638dcefccd8e3be
证书SHA256: 81c56776b47c3435914dcdb81c7a7eb6449a6c80151d350912dfff0c9a88de1b
证书SHA512:
481cf7bbd848c66f09c710b58407f12dd47ba4e239fdaa843216540e18ae43850197e29427f710b8ff339ad9d8a0f0e5fc693741a09a910cd9524da950e832e4

公钥算法: rsa
密钥长度: 2048
指纹: abf74915a71c9200eeb09b2cf061dfd26e97ee013de28a862776b2e7d4152a3b
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.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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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。
com.jf.gk.client.permission.JPUSH_MESSAGE	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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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_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.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.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_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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后台进程仍然运行。
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.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。
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.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
com.jf.gk.client.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.jf.gk.client.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.jf.gk.client.permission.MIPUSH_RECEIVE	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.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。

com.jf.gk.client.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.jf.gk.client.permission.C2D_MESSAGE	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。
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.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。

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	应用程序已使用代码签名证书进行签名

Manifest 配置安全分析

高危: **8** | 警告: **20** | 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。

3	Activity (com.jf.gk.client.StartActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
4	Service (com.jf.gk.client.service.KeepLiveService) 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。
5	Activity （com.huawei.hms.hmsscankit.ScanKitActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
6	Activity （com.jf.gk.client.ui.main.MainActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
7	Activity （com.tencent.liteav.trtccalling.ui.base.BaseCallActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
8	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.jf.gk.client.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
9	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.jf.gk.client.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
10	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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。
11	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
12	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。

本报告由南明离火移动安全分析平台生成

13	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。
14	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。
15	Service (com.meizu.cloud.pushsdk.NotificationService) 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	Broadcast Receiver (com.meizu.cloud.pushsdk.MzPushSystemReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.meizu.flyme.permission.PUSH [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。
17	Broadcast Receiver (cn.jpush.android.service.PluginMeizuPlatformsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.meizu.flyme.permission.PUSH [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。
18	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.push.permission.UPSTAGESERVICE [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。
19	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。
20	Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) 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。

本报告由南明离火移动安全分析平台生成

21	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。
22	Activity (cn.jpush.android.ui.PopWinActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
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) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
25	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。
26	Activity (cn.jpush.android.service.JNotifyActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
27	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。
28	Activity (cn.android.service.JTransitActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
29	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。
30	Service (com.blankj.utilcode.util.MessengerUtils$ServerService) 未被保护。 存在一个 intent-filter。	警告	发现 Service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Service是显式导出的。
31	高优先级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: **7** | 警告: **7** | 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	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	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
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
7	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
8	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

9	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
10	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
11	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
12	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
13	使用弱加密算法	高危	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	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
15	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
16	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

17	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	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/libggml.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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。 该对于Dart/Flutter库不适用，除非使用了Dart FFI	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

2	arm64-v8a/libtxsoundtouch.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	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning 符号可用

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_SMS android.permission.CALL_PHONE android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.READ_PHONE_STATE android.permission.GET_TASKS
其它常用权限	13/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.BLUETOOTH android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.REORDER_TASKS android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_BACKGROUND_LOCATION

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
glpt.neea.edu.cn	安全	是	**IP地址:** 121.194.8.35 **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
realm.io	安全	否	**IP地址:** 18.67.51.10 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.271179 **经度:** 127.442421 **查看:** Google 地图
itsm.jf-r.com	安全	是	**IP地址:** 101.207.142.35 **国家:** 中国 **地区:** 四川 **城市:** 成都 **纬度:** 30.666670 **经度:** 104.066269 **查看:** 高德地图
glpt-pre.neea.edu.cn	安全	是	**IP地址:** 121.194.8.35 **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
docs.mongodb.com	安全	否	**IP地址:** 146.75.50.133 **国家:** 瑞典 **地区:** 西约塔兰省 **城市:** 哥德堡 **纬度:** 57.707409 **经度:** 11.966732 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://itsm.jf-r.com:53800	自研引擎-A
• javascript:setandroidscrla • javascript:getandroiddata • javascript:setpagestatus	com/jf/gk/client/ui/main/WebFragment.java
• https://realm.io/docs/java/latest/#rxjava	io/realm/RealmObject.java
• https://testdatalbs.sparta.html5.qq.com/tr?wf4	c/t/m/g/cz.java
• https://testdatalbs.sparta.html5.qq.com/tr?utr	c/t/m/g/cy.java

• https://glpt.neea.edu.cn:8090/ • https://glpt.neea.edu.cn:8090/imapi • wss://glpt.neea.edu.cn:8090/appws	com/jf/gk/client/BuildConfig.java
• file:buf:	c/t/m/g/cw.java
• https://testdatalbs.sparta.html5.qq.com/tr?sf	c/t/m/g/db.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java
• http://callback	io/openim/android/ouicore/utils/Constant.java
• javascript:getandroiddata	com/jf/gk/client/ui/main/X5WebFragment.java
• https://img0.baidu.com/it/u=1049144354,3589714554&fm=253&fmt=auto&app=120&f=jpeg?w=1280&h=800	com/jf/gk/client/widget/SwipeCaptchaDialog.java
• 3.5.1.62	c/t/m/g/n.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• https://github.com/realm/realm-java/tree/master/examples/rxjavaexample • https://docs.mongodb.com/realm/sdk/android/install/#customize-dependencies-defined-by-the-realm-gradle-plugin	io/realm/RealmConfiguration.java
• https://glpt.neea.edu.cn:10000 • https://itsm.jf-r.com:53800/ • http://10.111.4.211:443/ • wss://glpt-pre.neea.edu.cn:30001 • https://itsm.jf-r.com:54002 • https://glpt-pre.neea.edu.cn:443/imapi • ws://10.111.4.211:30001 • https://glpt-pre.neea.edu.cn:443/ • wss://itsm.jf-r.com:54001 • wss://glpt.neea.edu.cn:17778 • http://10.111.4.211:30002 • https://glpt.neea.edu.cn/	io/openim/android/ouicore/utils/URLConstant.java
• javascript:webviewjavascriptbridge._fetchqueue • javascript:webviewjavascriptbridge	com/github/lzyzsd/jsbridge/BridgeUtil.java
• javascript:webviewjavascriptbridge._fetchqueue	com/github/lzyzsd/jsbridge/BridgeWebView.java
• https://github.com/vinc3m1/roundedimageview • https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Golang	Google	Go 是一种开源编程语言，可轻松构建简单，可靠和高效的软件。

IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
腾讯云通信 SDK	Tencent	腾讯云通信基于 QQ 底层 IM 能力开发，仅需植入 SDK 即可轻松集成聊天、会话、群组、资料管理能力，帮助您实现文字、图片、短语音、短视频等富媒体消息收发，全面满足通信需要。
360 加固	360	360 加固保是基于 360 核心加密技术，给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。
腾讯云短视频 SDK	Tencent	腾讯云点播推出了短视频一站式解决方案，覆盖了视频生成、上传、处理、分发和播放在内的各个环节，帮助用户以最快速度实现短视频应用的上线。
腾讯地图 SDK	Tencent	腾讯地图定位 SDK 是一套基于 Android 4.1 及以上版本设备的应用程序接口，通过该接口，您可以轻松使用腾讯地图定位服务，构建 LBS 应用程序。
Realm	Realm	Realm 平台是一个用于跨平台应用程序的次世代数据层。Realm 是可嵌式的、并发的和轻量级的，它允许您使用实时的原生对象。使用 Realm 可使您的应用程序在信号较弱、脱机或中断的情况下无缝运行。
HMS Scan Kit	Huawei	统一扫码服务（Scan Kit）提供便捷的条形码和二维码扫描、解析、生成能力，帮助您快速构建应用内的扫码功能。得益于华为在计算机视觉领域能力的积累，Scan Kit 可以实现远距离/小型码的检测和自动放大，同时针对常见复杂扫码场景（如反光、暗光、污损、模糊、弯曲）做了针对性识别优化，提升扫码成功率与用户体验。Scan Kit 支持 Android 和 iOS 系统集成，其中，Android 系统集成 Scan Kit 后支持横屏扫码能力。
腾讯云实时音视频 SDK	Tencent	实时音视频（Tencent RTC）基于腾讯多年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
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。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
HMS Core	Huawei	HMS Core 是华为为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
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。
Matisse	Zhihu	一个设计精美的 Android 图片视频选择器。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。

HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
HMS ML Kit	Huawei	机器学习服务（ML Kit）提供机器学习套件，为开发者使用机器学习能力开发各类应用，提供优质体验。得益于华为长期技术积累，ML Kit 为开发者提供简单易用、服务多样、技术领先的机器学习能力，助力开发者更快更好地开发各类 AI 应用。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。
OPPO Push	OPPO	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

邮箱地址敏感信息提取

EMAIL	源码文件
a@qq.com	io/openim/android/ouicore/widget/DebugActivity.java

第三方追踪器检测

名称	类别	网址
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
WeChat Location		https://reports.exodus-privacy.eu.org/trackers/76

敏感凭证泄露检测

可能的密钥
vivo推送的=> "com.vivo.push.app_id" : "105559740"
极光推送的=> "JPUSH_APPKEY" : "d21f5f120cdcc32c8d220268"
vivo推送的=> "com.vivo.push.api_key" : "9a76ba[illegible]a7[illegible]e46f61c1e9f6e5d2b7fd1"
OPPO推送的=> "OPPO_APPID" : "30886492"
OPPO推送的=> "OPPO_APPSECRET" : "436c6422ccc04efe8a18d28a06a9adbb"
极光推送的=> "JPUSH_CHANNEL" : "developer-default"
腾讯位置服务的=> "TencentMapSDK" : "CXOBZ-SI36B-MSKU4-J7FN4-IEMBE-KYB5C"
华为HMS Core应用ID的=> "com.huawei.hms.client.appid" : "appid=107114073"
魅族推送的=> "MEIZU_APPID" : "148396"
荣耀推送的=> "com.hihonor.push.app_id" : "100100147"

魅族推送的=> "MEIZU_APPKEY" : "cf21a4c6b2934c5bb4f5dcecdf681c22"
OPPO推送的=> "OPPO_APPKEY" : "7a5e746b6bf24cd0889ef244b167d831"
小米推送的=> "XIAOMI_APPKEY" : "MI-5532015778153"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDM0LDMzLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
小米推送的=> "XIAOMI_APPID" : "MI-2882303761520157153"
"is_private_chat" : "is_private_chat"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
eyJVSUQiOiJhQHFxLmNvbSIsIlBsYXRmb3JtIjoiQW5kcm9pZCIsImV4cCI6MTk2ODYzOTQxOSwibmJmIjoxNjUzMjc5NDE5LCJpYXQiOjE2NTMyNzk0MTI9
FDA50693-A4E2-4FB1-AFCF-C6EB07647825
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D1
c731a0c3176036fc0482313939070e5df1a7ebadf2084292d2e0155b9b022714
AB8190D5-D11E-4941-ACC4-42F30510B408
15f1483824cf4085ddca5a8529d873fc59a8ced2cbce67fb2b3dd9033ea03442
5e1fe70424035ee83066ac22b24f31dc

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。