南明离火
移动应用检测平台

ANDROID 静态分析报告

沁石轩 • v1.7.8

分析日期: 2024-05-14 10:55:16

应用概览

文件名称:	base.apk
文件大小:	52.03MB
应用名称:	沁石轩
软件包名:	edf89.biadiga
主活动:	com.netease.nim.main.main.activity.WelcomeActivity
版本号:	1.7.8
最小SDK:	21
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	0e4dd0ff07929460aa9003f8db6931cb
SHA1:	6d300c11d283c3c1415e697ba[illegible]0f6ade289
SHA256:	6e8a6d153be3c4eefe0b2[illegible]ddec217f579f53957911

分析结果严重性分布

高危	中危	信息	安全	关注
5	30	2	1	11

四大组件导出状态统计

Activity组件：160个，其中export的有： 3个
Service组件：28个，其中export的有： 9个
Receiver组件：16个，其中export的有： 7个
Provider组件：3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: C=sign.keysboejgetore, ST=sign.keysboejgetore, L=sign.keysboejgetore, O=sign.keysboejgetoresign.keysboejgetore, OU=sign.keysboejgetore, CN=sign.keysboejgetore
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-19 06:31:27+00:00
有效期至: 2025-03-14 06:31:27+00:00
发行人: C=sign.keysboejgetore, ST=sign.keysboejgetore, L=sign.keysboejgetore, O=sign.keysboejgetoresign.keysboejgetore, OU=sign.keysboejgetore, CN=sign.keysboejgetore
序列号: 0x6ac1f463
哈希算法: sha256
证书MD5: 640477d014e21ab4873ed6cb64194256
证书SHA1: e813c15f64ad27de11388ad1119e6c6062992b41
证书SHA256: 00a87d059ecb72f08fcb95bc32a94e7ed50fa6103cf66a8a99899307ac1ef846
证书SHA512: 4562619a22d4b20d807032b41a637c990a3fa503aa5d5601dc4f0f7fc73cb094d71a03b1dc00d475e23192a89250fd5fb268c59b564ca2f7201ab64cf23beb4a

公钥算法: rsa
密钥长度: 1024
指纹: f167e451538f0c9fb0c6e835f56259b1d23afa82289621609c21ad1287260a65
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.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.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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
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_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.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.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.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）
edf89.biadiga.permission.RECEIVE_MSG	未知	未知权限	来自 android 引用的未知权限。
edf89.biadiga.permission.MIPUSH_RECEIVE	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。
edf89.biadiga.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。
edf89.biadiga.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.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。
edf89.biadiga.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
edf89.biadiga.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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。
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.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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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。
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.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。
android.permission.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
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_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_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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

本报告由南明离火移动安全分析平台生成

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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.netease.nim.main.main.activity.WelcomeActivity	Schemes: easychat://,
com.netease.nim.main.main.activity.MixPushActivity	Schemes: pushscheme://, Hosts: com.huawei.codelabpush, Paths: /deeplink,
com.netease.yunxin.nertc.nertcvideocall.push.SignallingHuaweiPushActivity	Schemes: pushscheme://, Hosts: com.netease.nimlib.avsignalling.push, Paths: /huawei,

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: **0** | 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	Service (com.netease.nimlib.job.NIMJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。

4	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。
5	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。
6	Broadcast Receiver (com.netease.nimlib.mixpush.mi.MiPushReceiver) 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。
7	Activity (com.netease.nim.main.main.activity.MixPushActivity) 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。
8	Broadcast Receiver (com.netease.nimlib.mixpush.mz.MZPushReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
9	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。
10	Broadcast Receiver (com.netease.nimlib.mixpush.vivo.VivoPushReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
11	Service (com.netease.nimlib.mixpush.oppo.OppoPushService) 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。
12	Service (com.netease.nimlib.mixpush.oppo.OppoAppPushService) 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。

本报告由南明离火移动安全分析平台生成

13	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。
14	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。
15	Activity (com.netease.yunxin.nertc.nertcvideocall.push.SignallingHuaweiPushActivity) 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。
16	Activity (com.netease.yunxin.nertc.nertcvideocall.push.SignallingOppoPushActivity) 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。
17	Broadcast Receiver (com.netease.yunxin.nertc.nertcvideocall.service.NotificationBroadcastReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
18	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: edf89.biadiga.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Broadcast Receiver 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。
19	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: edf89.biadiga.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Broadcast Receiver 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。

20	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。
21	Content Provider (com.huawei.hms.support.api.push.PushProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: edf89.biadiga.permission.PUSH_PROVIDER protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Content Provider 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。
22	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。
23	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。
24	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。

代码安全漏洞检测

高危: **5** | 警告: **8** | 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
3	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限

4	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
5	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
6	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
7	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
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	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
10	SHA-1是已知会受冲突的弱哈希	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
11	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

12	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
13	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
14	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
15	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
16	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	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-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/librts_network.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: ['__FD_CLR_chk', '__FD_SET_chk', '__FD_ISSET_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	11/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.GET_TASKS android.permission.VIBRATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	15/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.BLUETOOTH android.permission.BROADCAST_STICKY

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

nim-sdk.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美利坚合众国 **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
qy-swallow.qiyukf.com	安全	是	**IP地址:** 183.136.182.36 **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
appgallery.cloud.huawei.com	安全	是	**IP地址:** 183.136.182.36 **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
mpush-api.aliyun.com	安全	是	**IP地址:** 183.136.182.36 **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
qydev.netease.com	安全	是	**IP地址:** 59.111.48.68 **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
da.qiyukf.netease.com	安全	是	**IP地址:** 59.111.222.254 **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
da.qytest.netease.com	安全	是	**IP地址:** 59.111.241.137 **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
nim.qiyukf.com	安全	是	**IP地址:** 183.136.182.36 **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

qytest.netease.com	安全	是	**IP地址:** 183.136.182.36 **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
qiyukf.netease.com	安全	是	**IP地址:** 59.111.222.254 **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
api-collection2.jrmf360.com	安全	否	No Geolocation information available.
api2.jrmf360.com	安全	否	No Geolocation information available.
store.hispace.hicloud.com	安全	是	**IP地址:** 183.136.182.36 **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
da.qiyukf.com	安全	是	**IP地址:** 183.136.182.36 **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
yun-test2.jrmf360.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://www.163.com/1.jpg	自研引擎-A
• 127.0.0.1 • http://%s:%d/%s	com/a/a/f.java
• http://%s:%d/%s	com/a/a/k.java
• https://mpush-api.aliyun.com/v2.0/a/audid/req/	com/c/a/d/h.java
• https://api2.jrmf360.com/ • https://yun-test2.jrmf360.com/	com/jrmf360/normallib/JrmfClient.java
• https://api-collection2.jrmf360.com/api/v1/mobiledate/collectdata.shtml	com/jrmf360/normallib/rp/http/RpHttpManager.java
• https://api-collection2.jrmf360.com/api/v1/mobiledate/collectdata.shtml	com/jrmf360/normallib/wallet/http/WalletHttpManager.java

• http://qytest.netease.com • http://qiyukf.netease.com • http://qydev.netease.com • https://nim.qiyukf.com • https://qy-swallow.qiyukf.com • http://da.qytest.netease.com • http://da.qiyukf.netease.com • https://da.qiyukf.com	com/qiyukf/unicorn/ysfkit/unicorn/i/b/a.java
• https://nim-sdk.firebaseio.com • https://play.google.com/store/apps/details?id= • https://appgallery.cloud.huawei.com/app/ • https://play.google.com/store • https://appgallery.cloud.huawei.com	自研引擎-S
• 127.0.0.1	lib/arm64-v8a/libnls_network.so

Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 之上作为运行原生代码。
网易云信	Netease	网易云信致力于互联网络技术的开发与研究，使开发者通过简单集成客户端 SDK 和云端开放 API，快速实现强大的移动互联网 IM 和音视频功能。
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。
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。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
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。
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。
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。
HMS Core	Huawei	HMS Core 是华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。
HMS Update	Huawei	用于 HMS SDK 引导升级 Huawei Mobile Services(APK)，提供给系统安装器读取升级文件。
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。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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。
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来载返回。
网易云通信 SDK	Netease	IM SDK 是网易云通信其他能力（实时语音视频、互动白板等）的基础，本节讲述 IM SDK 的集成步骤也将其他能力 SDK 的集成步骤融合起来，开发者可以根据实际业务需要选择接入的类库。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 Media2 取代。
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。
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。

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
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

敏感凭证泄露检测

可能的密钥

网易云信 IM SDK的=> "com.netease.nim.appKey" : "b8aa47e5b25892141666583bc99bad1b"
vivo推送的=> "com.vivo.push.api_key" : "2e8c38a8-604a-4c96-9bc0-e102f72728e9"
"nrtc_setting_voe_call_proximity_key" : "nrtc_setting_voe_call_proximity_key"
"nrtc_setting_vie_quality_key" : "nrtc_setting_vie_quality_key"
"nrtc_setting_vie_crop_ratio_key" : "nrtc_setting_vie_crop_ratio_key"
"main_tab_session" : "percakapan"
"nrtc_setting_vie_default_front_camera_key" : "nrtc_setting_vie_default_front_camera_key"
"nrtc_setting_other_device_default_rotation_key" : "nrtc_setting_other_device_default_rotation_key"
"team_authentication" : "Autentikasi"
"nrtc_setting_voe_audio_ns_key" : "nrtc_setting_voe_audio_ns_key"
"google_api_key" : "AIzaSyCL6S3DSVG3nTZjDr4UwKZQMB8NwL3Lgog"
"nrtc_setting_voe_high_quality_key" : "nrtc_setting_voe_high_quality_key"
"nrtc_setting_voe_audio_aec_key" : "nrtc_setting_voe_audio_aec_key"
"nrtc_setting_vie_max_bitrate_key" : "nrtc_setting_vie_max_bitrate_key"
"nrtc_setting_other_device_rotation_fixed_offset_key" : "nrtc_setting_other_device_rotation_fixed_offset_key"
"nrtc_setting_vie_hw_encoder_key" : "nrtc_setting_vie_hw_encoder_key"
"nrtc_setting_other_server_record_video_key" : "nrtc_setting_other_server_record_video_key"
"team_authentication" : "Authentication"
"nrtc_setting_vie_rotation_key" : "nrtc_setting_vie_rotation_key"
"nrtc_setting_vie_hw_decoder_key" : "nrtc_setting_vie_hw_decoder_key"
"nrtc_setting_other_server_record_audio_key" : "nrtc_setting_other_server_record_audio_key"
"google_crash_reporting_api_key" : "AIzaSyCL6S3DSVG3nTZjDr4UwKZQMB8NwL3Lgog"
"nrtc_setting_vie_fps_reported_key" : "nrtc_setting_vie_fps_reported_key"
"main_tab_session" : "conversation"
"firebase_database_url" : "https://nim-sdk.firebaseio.com"
d80f18e8081b624cc64985f87f7011bf1702985d2e10dbc985ee7be334fd3c7d
173cf86fe9894a0f70daadd094fd88c380836099d4939f8c3754361bdc16a32b
4bdecdf772491e75c4d8b48f88aee22bae1311984f2e1da4dfad0b78ee7f5163
QrMgt8GGYK752ZY5AnhtxkLzb8egpFn3j5JELI8H6wtACbUnZ5cc3aYTsTRbmkAkRJeYbtx92LPBWm7nBO9Ull7y5i5MQNmUZNf5QENurR5tGyo7yJ2G0MBjWvy6iAtlAbacKP0SwOUeUWx5dsBdyhxa7ld1APtybSdDgicBDuNjI0mlZFUzZSS9dmN8lBD0WTVOMz0pRZbR3cysomRXOO1ghqjJdTcyDIxzpNAEszN8RMGjrzyU7Hjbmwi6YNK

92974c6802419e4d18b5ec536cbfa167b8e8eff09ec4c8510a5b95750b1e0c82
5fed96c85bd58c58aadbd465c172a4c9a794d8eb2f86cbc7bcee6caf4c7a2c5f
403f14ad2f0e5eb3c4f3a0bcd5c1592cc4492662ad53191c92905255d4990656
db53fcdc9ab71e9bdd4eab257fe1aba7989ad2b24fbe3a85dfef72ea1dd6bae2
b368b110e3b565fe97c91f786e11bc48754cc8e4e6f21d8a94a68ac6ad67aaaf
3081a0adab3018d57165e6dd24074bdbac640f6dbe21a9e24d3474a87ebf38b8
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a15cc760cd3604af8d57f0e0c693cc
db48223fd9e143f7e133c57f5d08a4e38549ce3ebd921fe3b4003c26e5e35bed
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn
4230baa077b401374d0fc012375047e79ea0790d58d095ef18d97d95470c738d
07ff9b7aeeff969173c45b285fe0fecdbaae244576ff7a2796a36f1c0c11adb4
e2f856b9f9a4fd4cb2795aeaf83268e4bff189aaec05d691ffde76e075b82648

免责声明及风险提示: