南明离火
移动应用检测平台

ANDROID 静态分析报告

鹅圈子 • v1.0.10

分析日期: 2024-07-24 14:46:28

应用概览

文件名称:	鹅圈子.apk
文件大小:	89.84MB
应用名称:	鹅圈子
软件包名:	com.xet.community
主活动:	com.xiaoe.circle.app.core.ui.splash.SplashActivity
版本号:	1.0.10
最小SDK:	21
目标SDK:	30
加固信息:	腾讯云移动应用安全（腾讯御安全） 加固
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	5/432
杀软检测:	AI评估：可能有安全隐患
MD5:	d8413d9f421672502b9c573b792f7c35
SHA1:	b311e5acdbb5be5407479219181f892ce5a01c6c0
SHA256:	8782c98810aaafde1dca9ab69fd651c52c1892fc384bfc67b11bbe1edb6c49db

分析结果严重性分布

高危	中危	信息	安全	关注
7	29	3	1	12

四大组件导出状态统计

Activity组件：42个，其中export的有： 12个
Service组件：21个，其中export的有： 7个
Receiver组件：11个，其中export的有： 3个
Provider组件：6个，其中export的有： 2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: True
v4 签名: False
主题: C=86, ST=Guangdong, L=Shenzhen, O=Xiaoe Technology, OU=App Development Team, CN=Xiaoe Merchant
签名算法: rsassa_pkcs1v15
有效期自: 2019-07-08 08:05:31+00:00
有效期至: 2049-06-30 08:05:31+00:00
发行人: C=86, ST=Guangdong, L=Shenzhen, O=Xiaoe Technology, OU=App Development Team, CN=Xiaoe Merchant
序列号: 0x15781a8b
哈希算法: sha256
证书MD5: 87178f2908a2f134d1b0a0a9b28b2d0b
证书SHA1: 4394ea11ca2f90f1948c26bb1fe80b129ab8eb40
证书SHA256: 6cf5794cbe67c0da9c94e39792cfc05310484f7aa12367a06d5838ab9538067b
证书SHA512:
27bea3ac112003c7edf06e43f4c69d5335d114f080a8f258d5924942dc2c0a3c53c4c434c63cd832eeebf795bb7a88f186097c3b77e79ada535a66e67d9b74c6

公钥算法: rsa
密钥长度: 2048
指纹: 10a524c11f355c9c3d35b3016ac843ce84ab98f2a19570d85ba92fb767fdf785
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.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.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.ACCESS_ALL_DOWNLOADS	未知	未知权限	来自 android 引用的未知权限。
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_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.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_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.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。
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.xet.community.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。
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.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
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.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.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。
READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息，这样应用程序可以发现您的手机使用情况，这些信息可能包含用户个人信息或保密信息，造成隐私数据泄露。
com.xet.community.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.xet.community.permission.PUSH_PROVIDER	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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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.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。
com.xet.community.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.xet.community.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.xet.community.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.xiaoe.circle.app.core.ui.splash.SplashActivity	Schemes: xetecommunity://,

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: **29** | 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.xiaoe.circle.ui.course.activity.CircleMainActivity) 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。
4	Broadcast Receiver (cn.jpush.android.service.PushReceiver) 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。
5	Activity (com.xiaoe.base.push.vendor.XEPushVendorActivity) 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。
6	Activity 设置了 TaskAffinity属性 (com.xiaoe.base.wechat.login.LoginMiddleWareActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名

7	Activity (com.xiaoe.base.wechat.login.LoginMiddleWareActivity) 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。
8	Activity-Alias (com.xet.community.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
9	Activity设置了TaskAffinity属性 (com.xiaoe.base.wechat.pay.PayMiddleWareActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity (com.xiaoe.base.wechat.pay.PayMiddleWareActivity) 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。
11	Activity-Alias (com.xet.community.wxapi.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.xet.community.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
13	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.xet.community.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
14	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。
15	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。
16	Service (com.meizu.cloud.push.MzNotificationService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.meizu.cloud.push.permission.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

17	Content Provider (com.billy.cc.core.component.remote.RemoteProvider) 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。
18	Activity设置了TaskAffinity属性 (com.billy.cc.core.component.remote.RemoteConnectionActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
19	Activity (com.billy.cc.core.component.remote.RemoteConnectionActivity) 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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	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。
27	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。

28	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。
29	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。
30	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。
31	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。
32	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: **6** | 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	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	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

3	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
4	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
5	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
6	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
7	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
8	不安全的Web视图实现。WebView忽略SSL证书错误并接受任何SSL证书。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
9	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
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	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	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
13	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
14	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
15	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
16	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
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
18	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
19	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	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/libtquic_jni.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：['__memcpy_chk', '__strcpy_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_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	8/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION

本报告由南明离火移动安全分析平台生成

其它常用权限	10/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT com.google.android.gms.permission.AD_ID 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
v3.wufazhuce.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图
h5-pay.inside.xiaoeknow.com	安全	是	**IP地址:** 119.29.39.84 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
www.xiaoe-tech.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
sensors.xeknow.com	安全	是	**IP地址:** 101.226.137.106 **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
admin.xiaoe-tech.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图

h5-pay.sdk.inside.xiaoe-tech.com	安全	是	**IP地址:** 134.175.39.17 **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
vodreport.qcloud.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
admin-mobile.xiaoeknow.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
community-app.xiaoeknow.com	安全	是	**IP地址:** 101.226.137.106 **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
h5-pay.sdk.test.xiaoe-tech.com	安全	是	**IP地址:** 123.207.112.148 **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
api-push.in.meizu.com	安全	否	**IP地址:** 206.161.233.191 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 赫恩登 **纬度:** 38.978210 **经度:** -77.386993 **查看:** Google 地图
wx.tenpay.com	安全	是	**IP地址:** 101.226.137.106 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
h5-pay.sdk.xiaoe-tech.com	安全	是	**IP地址:** 61.160.209.75 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://admin.xiaoe-tech.com/sdk_list_page • https://app.inside.xiaoe-tech.com/ • http://xiaoeapp-server.test.xiaoeknow.com/ • http://app.inside.xiaoe-tech.com/ • https://admin-mobile.test.xiaoeknow.com • http://xiaoeapp-assitant.test.xiaoeknow.com/ • https://xiaoeapp-assitant.xiaoeknow.com/ • https://admin-mobile.xiaoeknow.com • http://xiaoeapp-assitant.xiaoeknow.com/ • http://bigclass.learnreport.xiaoeknow.com • https://admin-mobile.inside.xiaoeknow.com • https://xiaoeapp-server.xiaoeknow.com/ • https://app.xiaoe-tech.com/ • https://admin.xiaoe-tech.com/data_share_page • http://git.code.oa.com/SecurityResearchProject/ANTI-Reverse.git • http://xiaoeapp-server.xiaoeknow.com/	自研引擎-A
• 4.6.2.1	com/wrapper/proxyapplication/WrapperProxyApplication.java
• https://h5-pay.sdk.xiaoe-tech.com	com/xiaoe/shop/webcore/core/utils/SPUtils.java
• https://119.29.29.99/d?dn=	com/xiaoe/circle/ui/web/videoupload/impl/j.java
• https://h5-pay.sdk.test.xiaoe-tech.com • http://h5-pay.sdk.inside.xiaoe-tech.com	com/xiaoe/shop/webcore/core/MerchantApp.java
• javascript:webviewjavascriptbridge._fetchqueue • javascript:webviewjavascriptbridge	com/xiaoe/shop/webcore/core/bridge/JsBridgeUtil.java
• https://sensors.xeknow.com/sa?project=holder&token=holder	com/xiaoe/base/sensors/XESensors.java
• https://www.xiaoe-tech.com/?channel=1435-1360-1361-153228&from_click=xe_know_app_02	com/xiaoe/circle/ui/personal/activity/AboutUsActivity.java
• https://admin-mobile.xiaoeknow.com	com/xiaoe/base/config/d.java
• https://vodreport.qcloud.com/ugcupload_new	com/xiaoe/circle/ui/web/videoupload/impl/r.java
• https://api-push.in.meizu.com/garcia/api/client/	e4/a.java
• http://v3.wufazhuce.com:8000	x5/e.java
• https://community-app.xiaoeknow.com/ • http://119.29.27.212:8889/ • http://community-app.xiaoeknow.com/	com/xiaoe/circle/app/core/config/AppConfigDefault.java
• http://clients3.google.com/generate_204	com/github/pwittchen/reactivenetwork/library/rx2/internet/observing/strategy/b.java
• http://clients3.google.com/generate_204	com/github/pwittchen/reactivenetwork/library/rx2/internet/observing/a.java

• www.google.com	com/github/pwittchen/reactivenetwork/library/rx2/internet/observing/strategy/a.java
• http://10.10.30.93:5173/	com/xiaoe/circle/ui/web/debug/WebUIDebug.java
• http://10.10.30.93:5173/latest-offline-package.json	com/xiaoe/circle/ui/web/debug/a.java
• http://soft.imtt.qq.com/browser/tes/feedback.html	com/xiaoe/shop/webcore/core/XiaoEWeb.java
• https://wx.tenpay.com • http://h5-pay.inside.xiaoeknow.com/ • https://mclient.alipay.com	com/xiaoe/shop/webcore/core/utils/Constance.java
• http://10.10.30.93:5173/latest-offline-package.json	com/xiaoe/circle/ui/web/debug/BundleUpdateDebug.java
• https://admin.xiaoe-tech.com/sdk_list_page • https://admin-mobile.xiaoeknow.com • https://admin.xiaoe-tech.com/p/static_page/protocol/groupapp_protocol • 4.6.2.1 • https://admin.xiaoe-tech.com/p/static_page/protocol/groupapp_privacy_protocol_page • https://admin.xiaoe-tech.com/data_share_page • https://admin.xiaoe-tech.com/childprotect_protocol_page	自研引擎-S
• www.google.com	lib/arm64-v8a/libtquic_jni.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时响应用户反馈。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。

ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ，并且轻量和极度灵活。
XPopup	li-xiaojun	内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营效果、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥深远的价值。
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。
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，而不是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 或令牌通过此包中对应的类承载返回。
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。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。
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
xiaoeks@xiaoe-tech.com	自研引擎-S

第三方追踪器检测

名称	类别	网址

Bugly		https://reports.exodus-privacy.eu.org/trackers/190
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
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
小米推送的=> "XIAOMI_APPID" : "MI-2882303761520288755"
OPPO推送的=> "OPPO_APPSECRET" : "OP-a2a1e304309848429c66860f0b091b34"
OPPO推送的=> "OPPO_APPKEY" : "OP-84fc25436e1b494dad44b1a9b275b2e6"
vivo推送的=> "com.vivo.push.api_key" : "d3277d53ac6d0f542ceca2984118e43d"
vivo推送的=> "com.vivo.push.app_id" : "105710765"
荣耀推送的=> "com.hihonor.push.app_id" : "900833926"
极光推送的=> "JPUSH_CHANNEL" : "xiaoe"
小米推送的=> "XIAOMI_APPKEY" : "MI-5262028822755"
魅族推送的=> "MEIZU_APPID" : "MZ-152732"
OPPO推送的=> "OPPO_APPID" : "OP-31468747"
魅族推送的=> "MEIZU_APPKEY" : "MZ-214ef13b460a420fba2707dd5430d25f"
极光推送的=> "JPUSH_APPKEY" : "4199ff072f0ca9447ed6ae42"
vivo推送的=> "local_iv" : "MzMsMzQsMzIsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzMywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzNSwzMiwzMiwjQDM1LDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=109971787"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QIDAQAB"
2b3dd3cb73a81288651df167a2b4f1b8
cd60c0a9-4e3c-487c-a9b6-2406b143d91d
6551f10358a9eb5b0a080597
4a2ca769d79f4856b3bd982d30de790
59bd2d0f-8474-451d-9bee-3cca00182b31

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。