南明离火
移动应用检测平台

ANDROID 静态分析报告

Garden • v4.3.7

分析日期: 2025-04-10 12:53:39

应用概览

文件名称:	Garden v4.3.7.apk
文件大小:	41.41MB
应用名称:	Garden
软件包名:	com.touchte.garden
主活动:	com.wind.im.MainActivity
版本号:	4.3.7
最小SDK:	23
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	4/432
杀软检测:	15 个杀毒软件报毒
MD5:	27f55860138af8608db637fe1694a5a3
SHA1:	c7477a5179370d8f2b39f85b6f4d2e7da3b78245
SHA256:	d9215b57be0f99699c962b22e8a8df826282baaf3e235ee0ffca20699849dc1f

分析结果严重性

高危	中危	信息	安全	关注
5	40	2	1	12

四大组件信息

Activity组件：109个，其中export的有： 6个
Service组件：26个，其中export的有： 12个
Receiver组件：14个，其中export的有： 7个
Provider组件：12个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=pdPEHLx1eov5kx8S5pzB, ST=zW9kbcxGY8nzwJpNszM5, L=j0H5rMgw6NVSASJD5RKR, O=WNrQO8vMbORtEvYGjziQ, OU=pJDCpi5aCcima2SQXe2O, CN=eLBWnOlq5TFvDYWXqtqe
签名算法: rsassa_pkcs1v15
有效期自: 2023-04-24 23:22:33+00:00
有效期至: 2050-09-09 23:22:33+00:00
发行人: C=pdPEHLx1eov5kx8S5pzB, ST=zW9kbcxGY8nzwJpNszM5, L=j0H5rMgw6NVSASJD5RKR, O=WNrQO8vMbORtEvYGjziQ, OU=pJDCpi5aCcima2SQXe2O, CN=eLBWnOlq5TFvDYWXqtqe
序列号: 0x11be5319
哈希算法: sha256
证书MD5: b64be181e57c12edc049430ec8050c9e
证书SHA1: 7f2523402b8db75ef2e71255e14aee860ab7528e
证书SHA256: 66f81b1973c440c49ef5ec13fdcbf05640eba59b336f169fc9d1e7c52f1acd87
证书SHA512: 64566b3c47f40391000e588909bdea8873336dff1d9e08a05e12b9cf992b0e1bcf34b23558956ca0f9cf6ef820aeae3b640379025c959b4486570c153ba8ef69

找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.touchte.garden.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
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.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.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。

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.touchte.garden.permission.MIPUSH_RECEIVE	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.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.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.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.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.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.touchte.garden.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.touchte.garden.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
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_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.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.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
com.touchte.garden.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
android.permission.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。

com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
android.permission.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
com.imacapp.common.WindCommTransitActivity	Schemes: jmfcim://,

网络通信安全

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。

证书安全分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

MANIFEST分析

高危: **0** | 警告: **30** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	Activity设置了TaskAffinity属性 (com.imacapp.wxapi.WXEntryActivity)	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
3	Activity (com.imacapp.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。
4	Activity-Alias (com.touchte.garden.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。

5	Service (com.heytap.mcssdk.PushService) 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。
6	Service (com.heytap.mcssdk.AppPushService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.heytap.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。
7	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。
8	Broadcast Receiver (com.wind.im.push.receiver.VivoPushMessageReceiverImpl) 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.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。
10	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。
11	Broadcast Receiver (com.wind.im.push.receiver.XiaomiPushMessageReceiver) 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。
12	Broadcast Receiver (com.wind.im.push.receiver.MeizuPushServerMsgReceiver) 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。
13	Service (com.taobao.accs.ChannelService) 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。
14	Service (com.taobao.accs.data.MsgDistributeService) 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	Broadcast Receiver (com.taobao.accs.EventReceiver) 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。
16	Broadcast Receiver (com.taobao.accs.ServiceReceiver) 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。
17	Service (org.android.agoo.accs.AgooService) 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。
18	Broadcast Receiver (com.taobao.agoo.AgooCommondReceiver) 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。
19	Activity (com.imacapp.common.WindCommTransitActivity) 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	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。
21	Activity设置了TaskAffinity属性 (com.touchte.garden.wxapi.WXEntryActivity)	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
22	Activity (com.touchte.garden.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。
23	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。
24	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: com.touchte.garden.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。

本报告由南明离火移动安全分析平台生成

25	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: com.touchte.garden.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。
26	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。
27	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: com.touchte.garden.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。
28	Service (com.umeng.message.UmengIntentService) 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。
29	Service (com.umeng.message.XiaomiIntentService) 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。
30	Service (com.umeng.message.UmengMessageIntentReceiverService) 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。
31	Activity设置了TaskAffinity属性 (com.umeng.message.notify.UPushMessageNotifyActivity)	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
32	Activity设置了TaskAffinity属性 (com.umeng.message.UMessageNotifyActivity)	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
33	Activity-Alias (com.umeng.message.UMessageNotifyActivity) 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。
34	Activity设置了TaskAffinity属性 (com.umeng.union.UMBoardActivity)	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

本报告由南明离火移动安全分析平台生成

</> 安全漏洞检测

高危: 3 | 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	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	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
4	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
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	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
7	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
8	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
9	不安全的Web视图实现。Web视图忽略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

10	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
11	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
12	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
13	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: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
14	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

动态库分析

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/libnative-lib.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__vsprintf_chk', '__memmove_chk', '__memset_chk', '__fgets_chk', '__memcpy_chk', '__strcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

2	arm64-v8a/librtmp-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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	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。	True info 符号被剥离
3	arm64-v8a/libtnet-3.1.14.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strrchr_chk', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk']	True info 符号被剥离

行为分析

编号	行为	标签	文件
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限

00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限

00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.SYSTEM_ALERT_WINDOW android.permission.RECORD_AUDIO android.permission.VIBRATE
其它常用权限	10/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_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。

域名检测

域名	状态	中国境内	位置信息
material.io	安全	否	**IP地址:** 216.239.36.21 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

api2.e.kuaishou.com	安全	是	**IP地址:** 103.102.202.151 **国家:** 中国 **地区:** - **城市:** - **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
www.xiaohongshu.com	安全	是	**IP地址:** 115.238.190.59 **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
static.yximgs.com	安全	是	**IP地址:** 115.238.190.59 **国家:** 中国 **地区:** 浙江 **城市:** 宁波 **纬度:** 29.878410 **经度:** 121.549767 **查看:** 高德地图
yoda.kwd.inkuai.com	安全	是	**IP地址:** 117.92.139.41 **国家:** 中国 **地区:** - **城市:** - **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
httpdns.bcelive.com	安全	是	**IP地址:** 117.92.139.41 **国家:** 中国 **地区:** 河北 **城市:** 保定 **纬度:** 38.851109 **经度:** 115.490280 **查看:** 高德地图
p2.a.yximgs.com	安全	是	**IP地址:** 221.231.47.223 **国家:** 中国 **地区:** 江苏 **城市:** 盐城 **纬度:** 33.385559 **经度:** 120.125282 **查看:** 高德地图
appgallery.cloud.huawei.com	安全	是	**IP地址:** 117.92.139.41 **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
edith.xiaohongshu.com	安全	是	**IP地址:** 117.92.139.41 **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

p5.a.yximgs.com	安全	是	**IP地址:** 117.92.139.41 **国家:** 中国 **地区:** 江苏 **城市:** 连云港 **纬度:** 34.600025 **经度:** 119.166847 **查看:** 高德地图
apidns.kwd.inkuai.com	安全	是	**IP地址:** 117.92.139.41 **国家:** 中国 **地区:** - **城市:** - **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
login.sina.com.cn	安全	是	**IP地址:** 106.63.15.207 **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
sdk-open-phone.getui.com	安全	是	**IP地址:** 115.227.15.237 **国家:** 中国 **地区:** 浙江 **城市:** 嘉兴 **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图
t2.xiaohongshu.com	安全	否	No Geolocation information available.
sock.ianpei.com	安全	否	**IP地址:** 172.86.122.62 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.783058 **经度:** -96.806503 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://apt.weixin.qq.com/ • https://yapt.qq.com/	com/imacapp/wind/api/LoginService.java
• javascript:document.body.innerHtml=	com/imacapp/home/web/KitWebViewClient.java
• 127.0.0.1	com/wind/im/MainActivity.java
• 127.0.0.1	com/wind/im/BuildConfig.java

• https://43.226.164.41 • https://120.46.157.112:7002 • https://49.233.102.113:5333 • https://www.xiaohongshu.com/api/im/users/following/all • https://103.102.200.38:80 • https://183.232.58.240:21004 • https://49.51.177.180:5333 • http://p5.a.yximgs.com/uhead/ab/2022/05/22/01/bmjaymja1mjiwmtuzmjdfmji5nzuxotu2ov8xx2hkndc0xze0oq==_s.jpg • https://sdk-open-phone.getui.com/api.php?format=json&t=1 • https://edith.xiaohongshu.com/api/sns/v1/search/placeholder?is_new_user=true • https://t2.xiaohongshu.com/api/collect • https://static.yximgs.com/bs2/adminblock/treasure-1675409076903-xywwjlqm.png • https://login.sina.com.cn/visitor/signin • https://124.71.10.22:7002 • https://118.26.252.225:5222 • https://apidns.kwd.inkuai.com/label_resolve?label=kwai-api&biz=aegon-android • http://p2.a.yximgs.com/uhead/ab/2021/08/16/17/ • https://edith.xiaohongshu.com/api/sns/v1/system_service/config?launchtimes=9 • https://183.134.98.111:5224 • http://httpdns.bcelive.com/?dns=bd-origin.pull.yximgs.com,bd-adaptive-pull.live-voip.com,bd-adaptive-pull.video-voip.com,bd-adaptive.pull.yximgs.com,bd-origin-pull.live-voip.com,bd-origin-pull.video-voip.com,bd-p2p-pull.live-voip.com,bd-p2p-pull.video-voip.com,bd-p2p.pull.yximgs.com,bd-proxy.pull.yximgs.com,bd-pull.live-voip.com,bd-pull.video-voip.com,bd.pull.yximgs.com,bd.push.yximgs.com,d5-ks.a.kwimgs.com,p5-live.a.yximgs.com,p5.a.yximgs.com,v5-skvod.kwaicdn.com,v5-kwaicdn.com&type=a • https://175.24.251.189:5333 • https://api2.e.kuaishou.com/rest/e/load/styletemplate • https://183.134.98.75:5224 • https://183.134.98.34:5224 • https://yoda.kwd.inkuai.com • https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf • https://43.129.255.160:8081	com/fake/android/boot/CheckUntil.java
• www.instance	com/imacapp/message/vm/GroupRedPackFixedViewModel.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• https://material.io/design/components/dialogs.html#actions	com/afollestad/materialdialogs/MaterialDialog.java
• https://appgallery.cloud.huawei.com • https://appgallery.cloud.huawei.com/app/ • https://play.google.com/store/apps/details?id= • https://play.google.com/store	自研引擎-S
• https://sock.ianpei.com/stat/cr	lib/arm64-v8a/libnative-lib.so

第三方SDK

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，及时跟进用户反馈。

C++ 共享库	Android	在 Android 应用中运行原生代码。
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。
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。
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。
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 可以实时地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。
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。
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。
友盟推送	Umeng	基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户活跃，提高 App 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。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
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。

追踪器

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

密钥凭证

可能的密钥
aHR0cHM6Ly84LjEzNC4xNjAuMTcxOjM2NTcvbG9ncy9nZGFjbmZ1aTQ=
aHR0cHM6Ly9nYXJkY3dldC5vczFhaDQ3eWwzLmNvbToyMDk2L2xvZ3MvZ2RhY25mdWk0
aHR0cHM6Ly8xMjAuNzguNzcuMzA6MzY1Ny9sb2dzL2dkYWNuZnVpNA==
aHR0cHM6Ly84LjEzNC42MC42OjM2NTcvbG9ncy9nZGFjbmZ1aTQ=
55e92a2be29cc6f1ea4d146fb9e6045d
f3423b38048b29b9e7bfec5c73e51ca1
aHR0cHM6Ly80Ny4xMDYuMjEzLjE3NzozNjU3L2xvZ3MvZ2RhY25mdWk0

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，不得用于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。