南明离火
移动应用检测平台

ANDROID 静态分析报告

ffakfak • v1.0.0.0

分析日期: 2025-04-30 21:55:51

应用概览

文件名称:	base.apk
文件大小:	4.68MB
应用名称:	ffakfak
软件包名:	build.ledear.fetps
主活动:	build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.MainActivity
版本号:	1.0.0.0
最小SDK:	21
目标SDK:	29
加固信息:	伪加密
开发框架:	Java/Kotlin
应用程序安全分数:	50/100 (中风险)
杀软检测:	15 个杀毒软件报毒
MD5:	3f6c743904e1735465f0bc6caa027360
SHA1:	5766fb12d8689e61d2b51053ba[illegible]2431e04f
SHA256:	7e5691af95ef9ec44a18f4590f47792f5dc56a71ffc9ca78c93f03950f7e6063

分析结果严重性

高危	中危	信息	安全	关注
1	41	0	1	0

四大组件信息

Activity组件：23个，其中export的有：24个
Service组件：9个，其中export的有：6个
Receiver组件：6个，其中export的有：6个
Provider组件：1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: None
主题: C=ThePhysioExp, ST=ThePhysioExp, L=ThePhysioExp, O=ThePhysioExp, OU=ThePhysioExp, CN=ThePhysioExp
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-27 17:53:13+00:00
有效期至: 2050-04-21 17:53:13+00:00
发行人: C=ThePhysioExp, ST=ThePhysioExp, L=ThePhysioExp, O=ThePhysioExp, OU=ThePhysioExp, CN=ThePhysioExp
序列号: 0x2d3e558b
哈希算法: sha256
证书MD5: fb1d325d45b65e039b427de7abc507a1
证书SHA1: e86b2c27f3258286c63a4edc4fcb5fa92d28c2cb
证书SHA256: 3894ee5973344bc05563744f759645994cc79e016be2c738de6e3fc9bbc1548b
证书SHA512:
838df0256b7d5061724a92c01727f6d777005a7243525d91337070959747fe2ebefd5b37ff77a1effb65b497e218cff41eba2a49fb5843f4d2d8626d472204fd

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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.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.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粗略的经纬度信息，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.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。
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.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_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.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.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。
oppo.permission.OPPO_COMPONENT_SAFE	签名	特定于 OPPO 设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。此权限可确保只有受信任的应用程序才能与 OPPO 系统的敏感部分进行交互。
oplus.permission.OPLUS_COMPONENT_SAFE	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.external_app_settings.USE_COMPONENT	签名	特定于华为设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。该权限确保只有受信任的应用才能与华为系统的敏感部分进行交互。
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.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.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.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.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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.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.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。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。

网络通信安全

序号	范围	严重级别	描述

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: **41** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup] 应该设置为false。默认情况下已被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Activity设置了TaskAffinity属性 (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.MainActivity)	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
4	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.MainActivity) 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。
5	Activity-Alias (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.SecondLauncherAlias) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
6	Activity-Alias (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.FirstLauncherAlias) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
7	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.sbxdxpjyykhbiazqzmesgedqrqatkbqvkievyjioiutmuqnemj20) 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 (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.FloatingView) 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。
9	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.pkhrcjcxqbenvbniwbwdolqbscicusresvctaltmzgrwlypjci4.CraxsBrowser) 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。
10	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.CameraActvity) 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 (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestScreenCap) 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。
12	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.SecondActivity) 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。
13	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.WakeupActivity) 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。
14	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestUninstall) 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	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestInstallPrim) 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。
16	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.installupdate) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

17	Broadcast Receiver (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ozyrgqmaxqlltmsltpxsjwadscbkybcqlkxdymldhqjtkzagll5.CustomReceiver) 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。
18	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.phhdhcbrkabgvmnncjmtmscfdzzkocrnrkyfjrnxdvcqnanmnf3.AccessService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_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。
19	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.phhdhcbrkabgvmnncjmtmscfdzzkocrnrkyfjrnxdvcqnanmnf3.BackgroundWorker) 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。
20	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.phhdhcbrkabgvmnncjmtmscfdzzkocrnrkyfjrnxdvcqnanmnf3.FirewallServices) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VPN_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。
21	Broadcast Receiver (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ozyrgqmaxqlltmsltpxsjwadscbkybcqlkxdymldhqjtkzagll5.BootReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [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。

22	Broadcast Receiver (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ozyrgqmaxqlltmsltpxsjwadscbkybcqlkxdymldhqjtkzagll5.PackagesReceiver) 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。
23	Activity设置了TaskAffinity属性 (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.flyActivity)	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
24	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.flyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
25	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.OpenActivity) 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 (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.OpenChrome) 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	Broadcast Receiver (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ozyrgqmaxqlltmsltpxsjwadscbkybcqlkxdymldhqjtkzagll5.ScreenReceiver) 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。
28	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.mnfcniuyxbsvojjedgcnfsjeuhglpmnbilcrabdagxbxbcvmxwzttre) 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	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.dmvdrxlxecjtmaoysiavafxlfdclilaszgrxuegdkeggrkl22Over) 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。

本报告由南明离火移动安全分析平台生成

30	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestDataUsage) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
31	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestVPN) 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。
32	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ukfmlrknvjqrgwkhpjbclcyulclqbdyxxyneelieyomwhacica29) 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。
33	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestOPPOB) 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。
34	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestKeyboard) 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。
35	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.glbywoeskwkfuhrynkjgfcprcijtdrcitwvggxmrcfknqrlifw21) 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。
36	Activity (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.RequestAdmin) 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。
37	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.phnidhcbrkabgvmpncjmtmsefdzzkocrnrkyfjrnxavcmanmnf3.MyJobService) 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。

本报告由南明离火移动安全分析平台生成

38	Broadcast Receiver (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.ozyrgqmaxqlltmsltpxsjwadscbkybcqlkxdymldhqjtkzagll5.Datareciver) 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。
39	Broadcast Receiver (build.ledear.AdminReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [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。
40	Service (build.ledear.akvbaumvfjwasfrhvvnkxndanqweqhzfnrbiiezeywbfwryfks2.phhdhcbrkabgvmnncjmtmscfdzzkocrnrkyfjrnxdvcqnanmnf3.KeyboardService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_INPUT_METHOD [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。
41	高优先级的Intent （999） - {2} 个命中 [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。

</> 安全漏洞检测

序号	问题	等级	参考标准	文件位置

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/libstringencryptionv3.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：['__memcpy_chk']	True info 符号被剥离

敏感权限分析

类型	匹配	权限
恶意软件常用权限	16/30	android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.READ_SMS android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	8/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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。

密钥证证

可能的密钥

谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "orlervotyrmxsydxwfdiycqdwzlbliwzmqsljjgngpjwhzkcca14"

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。