南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□□□

分析日期: 2025-07-05 16:33:56

应用概览

文件名称:	1231.apk
文件大小:	13.93MB
应用名称:	□□□□□
软件包名:	com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp
主活动:	com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.my.phone.ui.main.KeyPadActivity
版本号:	
最小SDK:	24
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:	47/100 (中风险)
跟踪器检测:	1/432
杀软检测:	17 个杀毒软件报毒
MD5:	9e1da03708ea8bc751885959e2d89fa8
SHA1:	38a687320411e83c33459da793e566697d74572a
SHA256:	ddb326ccbaff174ecc6ebc15ba0670e406ca61c3d0055b43d0b8807225700d05

分析结果严重性分布

高危	中危	信息	安全	关注
1	21	0	0	0

四大组件导出状态统计

Activity组件：31个，其中export的有： 8个
Service组件：16个，其中export的有： 3个
Receiver组件：12个，其中export的有： 4个
Provider组件：2个，其中export的有： 1个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=B, ST=K, L=S, O=T, OU=N, CN=U
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-09 17:45:47+00:00
有效期至: 2079-09-12 17:45:47+00:00
发行人: C=B, ST=K, L=S, O=T, OU=N, CN=U
序列号: 0x33ad4013a065865b
哈希算法: sha384
证书MD5: d508bddaca92beb5b52b562b766a57d5
证书SHA1: 6a0342c4edd7a0656520367d5a9281a21c4a70f1
证书SHA256: 8d974ab0e71c16c1f916ed719de0ab641f3820962b6987208eba703efb8b2cbf
证书SHA512:
e0cb5b20ea9f33c2f46cb491fe603cd252295a4e8ba8324f05b80b2b64260a16a59007335b1f2081be6d33c0f5b69addc5d895dcfc491d13914b5ffc6335469

公钥算法: rsa
密钥长度: 2048
指纹: ceacba94051f89a89d0a43b2bd21ee5badbb61eb861f2afcaf37aa3bf30d13e1
共检测到 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.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.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_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_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.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。

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.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.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.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.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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
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_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.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.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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.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.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.RECEIVE_LAUNCH_BROADCASTS	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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。

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.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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.my.phone.ui.calling.PhoneCallActivity	Schemes: tel://,

网络通信安全风险分析

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。

证书安全合规分析

高危: **0** | 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	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。

2	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
4	Activity (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Service (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.NotificationReServ) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
6	Activity (vpositronemissiontomographyscanner.asandaled.rburp.iunilateralism.prelativize.RmterminalleaveRgumresin) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Broadcast Receiver (com.aelectriccatfish.topiumaddict.swhiteseparatist.EghankXextensive) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问
8	Broadcast Receiver (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.cast.CallMyListener) 受权限保护，但应检查权限保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
9	Activity (com.vshillyshally.knhystaltopology.PhbathaspiragusPastronomer) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

10	Broadcast Receiver (com.ionychium.jrussula.znorthernalliance.ibride.JverosionGbc) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (cplover.kreadonlymemorychip.wfreedomofthepress.elastout.ssamuel.FmtautXconciseness) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
12	Activity 设置了 TaskAffinity 属性 (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.my.phone.ui.calling.PhoneCallActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
13	Activity (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.my.phone.ui.calling.PhoneCallActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Service (msantalales.ptremellareticulata.isectional.arondeau.ofairball.GaTremellaGrussianmonetaryunit) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
15	Broadcast Receiver (com.svoluptuously.yalphacentauri.ltiamat.UnoutsiderOteacloth) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
16	Content Provider (com.tgzpaiesn.bfejjblrhk.fvgejifrim.eoaepgs.puayckp.db.PackageContentProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
17	Service (hhonorific.kfreedomfromsearchandseizure.bmadagascar.qreport.culturist.cdysphoria.Cgsemiautomaticfirearm.QIakeonega) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。

18	Activity (com.ehydralazine.mpianist.ipanache.shybridtuberousbegonia.ScoutlineDsoapfilm) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
19	Activity (com.pstubbornness.idisaster.rkenning.EaccessibleSuprightActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
20	Activity (com.pstubbornness.idisaster.rkenning.KgratedcheeseOgeophyticActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
21	高优先级 Intent（2147483647） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	17/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.PROCESS_OUTGOING_CALLS android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.WRITE_CALL_LOG android.permission.WRITE_CONTACTS android.permission.VIBRATE

其它常用权限	10/46	android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.WRITE_EXTERNAL_STORAGE

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。

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，及时跟进用户反馈。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层用序列化/反序列化使用 protobuf 实现，性能高，稳定性强。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

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。