南明离火
移动应用检测平台

ANDROID 静态分析报告

• v1.3

本报告由南明离火移动安全分析平台生成

分析日期: 2024-07-18 14:48:24

应用概览

文件名称:	27a67eef65b4b0e50bbe4d98d31d4d048c5ee64f663fd5970f95c5c621fa2a5d.apk
文件大小:	13.3MB
应用名称:	
软件包名:	org.qnw.ojc.rckr
主活动:	com.learnpersecond.dailymassreading.PermissionActivity
版本号:	1.3
最小SDK:	26
目标SDK:	31
加固信息:	未加壳
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	2/432
杀软检测:	9 个杀毒软件报毒
MD5:	63d159211e77a805b24bda433ccd2295
SHA1:	f2a40cbdc4579361cbc253bb0409e4940071bff
SHA256:	27a67eef65b4b0e50bbe4d98d31d4d048c5ee64f663fd5970f95c5c621fa2a5d

分析结果严重性分布

高危	中危	信息	安全	关注
1	19	2	1	2

四大组件导出状态统计

Activity组件：27个，其中export的有： 1个
Service组件：14个，其中export的有： 4个
Receiver组件：12个，其中export的有： 4个
Provider组件：3个，其中export的有： 1个

应用签名证书信息

二进制文件已签名
v1 签名: True

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=CO
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-12 19:02:03+00:00
有效期至: 2024-07-16 10:38:03+00:00
发行人: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=CO
序列号: 0x4c901de9
哈希算法: sha256
证书MD5: 004a54891c84aacb1b2625c8f0e40b64
证书SHA1: b7e1374a0792dfd638e2e3300df2d01128caaf0c
证书SHA256: e2f749cd2ccfd160c229baa941bf1158cc914dc019caf87b49deeec759c06de5
证书SHA512:
317e7544e71f2aba3d20e09a805dbb8c9997552b105d65dc9bb2a466f216706ccc574cb8933712b2b70e9ea8cc6a93409f5acd27[illegible]b5b238b3d06b6df63b7306

公钥算法: rsa
密钥长度: 2048
指纹: 8b54a1ca2b7b8228f2963b7adc352e55bcf84ec6746cb1d8867ea91af92bf989
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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
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_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_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
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.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。
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）
org.qnw.ojc.rckr.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。
android.permission.READ_BASIC_PHONE_STATE	普通	允许对基本电话状态信息进行只读访问	允许只读访问具有非危险权限的手机状态，包括蜂窝网络类型、软件版本等信息。
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.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.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.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
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.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。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。

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: **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: **11** | 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存在漏洞的 Android 版本上 Android 8.0 [minSdk=26]	信息	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/custom_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。
4	Activity (com.learnpersecond.dailymassreading.Splash) 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	Service (androidx.work.impl.background.systemjob.SystemJobService) 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。
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。
8	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。
9	Content Provider (org.qnw.ojc.rckr.CvuVEw) 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。
10	Service (org.qnw.ojc.rckr.WAqDCA) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_TELECOM_CONNECTION_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。
11	Service (org.qnw.ojc.rckr.vDXFk) 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。
12	Broadcast Receiver (org.qnw.ojc.rckr.qrDTZb) 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。
13	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 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。

代码安全漏洞检测

高危: **0** | 警告: **6** | 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	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
3	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
4	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
5	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
6	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
7	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
8	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
9	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	4/30	android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	6/46	android.permission.INTERNET com.google.android.gms.permission.AD_ID android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.166 **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
admob-gmats.uc.r.appspot.com	安全	否	**IP地址:** 172.217.26.244 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.151.166 **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
googlemobileadssdk.page.link	安全	否	**IP地址:** 142.251.42.129 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图

g.co	安全	否	**IP地址:** 142.251.42.174 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
google.com	安全	否	**IP地址:** 172.217.26.238 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.251.42.142 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://fundingchoicesmessages.google.com/a/consent	AT0/l.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	J0/c.java
• https://googlemobileadssdk.page.link/ad-manager-android-update-manifest • https://googlemobileadssdk.page.link/admob-android-update-manifest	M0/L0.java
• www.google.com	L0/l.java
• https://firebase.google.com/support/privacy/init-options	Y2/C2813a.java
• https://goo.gl/naoooi • www.google.com • https://www.google.com	r1/g3.java
• https://app-measurement.com/a	r1/AbstractC2689v.java
• https://firebase.google.com/support/guides/disable-analytics	r1/C2703y1.java

• https://www.google.com/dfp/debugsignals • https://googlemobileadssdk.page.link/ad-manager-android-update-manifest • http://g.co/dev/packagevisibility • https://admob-gmats.uc.r.appspot.com/ • https://goo.gl/naoooi • https://app-measurement.com/a • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • www.google.com • https://firebase.google.com/support/guides/disable-analytics • https://fundingchoicesmessages.google.com/a/consent • https://www.google.com/dfp/senddebugdata • https://googlemobileadssdk.page.link/admob-interstitial-policies • https://firebase.google.com/docs/analytics • https://firebase.google.com/support/privacy/init-options • https://github.com/tink-crypto/tink-java • https://google.com/search? • https://googlemobileadssdk.page.link/admob-android-update-manifest • https://www.google.com/dfp/linkdevice • https://www.google.com • https://www.google.com/dfp/inapppreview • http://www.google.com • https://plus.google.com/ • https://pagead2.googlesyndication.com/pagead/ping?e=2&f=1	自研引擎-5

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
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，而不必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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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。
Jetpack Profileinstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。

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。

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-9273311230576901~4019310801"
"google_api_key" : "AIzaSyBeFyG4TN-1i23XWfl7-txjPEgeJ0-Ug1c"
"google_crash_reporting_api_key" : "AIzaSyBeFyG4TN-1i23XWfl7-txjPEgeJ0-Ug1c"
UGVybWl0aXIgYXBhcmVjZXIgZW5jaW1hIHBhcmEgY29udGludWFy
Q29uY2x1aXIgYSBpbnN0YWxhw6fDo28=
QXBwbGljYXRpb24gdW5hdmFpbGFibGUgaW4geW91ciByZWdpb24uIFRhcGA=TQsnIHRvIHJlbW92ZSBBcnA=
wr9QZXJtaXRpciBsYSBhcGFyaWNpw7NuIHNvYnJlIG90cmFzIGFwbGljYWNpb25lcz8=
UGVybWl0aXIgYXBhcmVjZXIgc29icmUgb3V0cm9zIHBhcmEgY29udGludWFy
QWxsb3cgZGlzcGxheSBvdmVyIG90aGVyIGFwcHMgdGhhdCBhcmU=
B3EEABB8EE11C2BE770B684D95219ECB
UGVybWl0aXIgYSBhcHJlc2VudGHDp8OjbyBzb2JyZSBvdXRyb3MgYXBsaWNhdGl2b3M/
QWxsb3cgZGlzcGxheSBvdmVyIG90aCVyIGFwcHM/

免责声明及风险提示: