南明离火
移动应用检测平台

ANDROID 静态分析报告

yxcalendar • v1.1.18

分析日期: 2024-07-01 12:21:21

应用概览

文件名称:	cn.youxiao.yxcalendar_1.1.18.apk
文件大小:	23.83MB
应用名称:	yxcalendar
软件包名:	cn.youxiao.yxcalendar
主活动:	cn.youxiao.yxcalendar.MainActivity
版本号:	1.1.18
最小SDK:	21
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：可能有安全隐患
MD5:	1f2a7b3c4f838492289facc8c3e65ea7
SHA1:	d1522f72ecbb2709018890b1df01e7dfb596cf74
SHA256:	c262dd2e379536d0f29ca84fee10673482deb08f98ba42e54736ada7d6014d

分析结果严重性分布

高危	中等	信息	安全	关注
0	29	1	0	3

四大组件导出状态统计

Activity组件：13个，其中export的有： 5个
Service组件：21个，其中export的有： 8个
Receiver组件：26个，其中export的有： 5个
Provider组件：8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

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=cn, ST=广东省, L=东莞市, O=优效软件工作室, OU=优效软件工作室, CN=游枭
签名算法: rsassa_pkcs1v15
有效期自: 2022-04-29 06:37:34+00:00
有效期至: 2049-09-14 06:37:34+00:00
发行人: C=cn, ST=广东省, L=东莞市, O=优效软件工作室, OU=优效软件工作室, CN=游枭
序列号: 0x59dbcb7a
哈希算法: sha256
证书MD5: b10c26e4f0a3472c19ac988a75f0103b
证书SHA1: 1df3ca32d77d7806a8d4c524a2083a391f0b40c4
证书SHA256: a5eb4761ed8d6fab59cbd6830661595e8f697e7fda07d3b7516120005cf9de9d
证书SHA512:
8dd97534b750c020425c1c3dc8da70635d8ec9cf08558d64e20b9bd3b80ef2733ad8fa4b90dad2984dbdd6f306725c223c7c52f1[illegible]059ce2db618119cbd09e31

公钥算法: rsa
密钥长度: 2048
指纹: 8c03120a0bbafb9d3ea5364e11332d95329a339977ea4624c2993e443a3436fd
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.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.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_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.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.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。
android.permission.USE_EXACT_ALARM	普通	允许在未经用户许可的情况下使用精确的警报	允许应用使用精确的警报。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
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.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。
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。
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.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.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）
cn.youxiao.yxcalendar.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
cn.youxiao.yxcalendar.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
cn.youxiao.yxcalendar.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
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.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。
cn.youxiao.yxcalendar.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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。

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: **26** | 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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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	Broadcast Receiver (cn.youxiao.yxcalendar.TodayWidget) 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。
4	Broadcast Receiver (cn.youxiao.yxcalendar.TodayCalendarWidget) 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。
5	Broadcast Receiver (cn.youxiao.yxcalendar.CalendarWidget) 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。
6	Activity设置了TaskAffinity属性 (com.jarvan.fluwx.wxapi.FluwxWXEntryActivity)	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设置了TaskAffinity属性 (cn.youxiao.yxcalendar.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
8	Activity-Alias (cn.youxiao.yxcalendar.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-Alias (cn.youxiao.yxcalendar.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。
10	Activity设置了TaskAffinity属性 (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	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
11	Service (androidx.glance.appwidget.GlanceRemoteViewsService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_REMOTEVIEWS [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	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。
13	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。
14	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: cn.youxiao.yxcalendar.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
15	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: cn.youxiao.yxcalendar.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
16	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。
17	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。
18	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。
19	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。

本报告由南明离火移动安全分析平台生成

20	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。
21	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。
22	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。
23	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。
24	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。
25	Broadcast Receiver (com.hihonor.push.sdk.PushReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: cn.youxinno.ycalendar.hihonor.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	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。
27	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。
28	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。

本报告由南明离火移动安全分析平台生成

29	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。
30	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: **0** | 警告: **1** | 信息: **1** | 安全: **0** | 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

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/libapp.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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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	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.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE 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
resolver.msg.xiaomi.net	安全	是	**IP地址:** 223.109.148.176 **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
ulogs.umengcloud.com	安全	是	**IP地址:** 223.109.148.176 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
cn.register.xmpush.xiaomi.com	安全	是	**IP地址:** 223.109.148.176 **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

goo.gle	安全	否	**IP地址:** 67.199.248.13 **国家:** 美利坚合众国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 6.0.4.101	自研引擎-M
• https://mp.weixin.qq.com/publicpoc/opensdkconf?action=getshareconf&appid=%s&sdkversion=%s&buffer=%s • 10.0.0.172 • https://resolver.msg.xiaomi.net/psc/?t=a • http://10.38.162.35:9085 • 3.0.0.7 • 111.202.1.252 • 10.0.2.15 • https://%1$s/gslb/?ver=5.0 • https://goo.gle/compose-feedback • 111.13.141.211 • 123.125.102.213 • 111.202.1.250 • https://play.google.com/store/apps/details?id= • file:///android_res/ • 10.38.162.35 • 39.156.81.172 • 111.13.142.153 • https://ulogs.umengcloud.com • https://cn.register.xmpush.xiaomi.com • www.baidu.com:80	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
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。
Jetpack Glance	Google	Build layouts for remote surfaces using a Jetpack Compose-style API.
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。
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。

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。
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。
荣耀推送服务	HONOR	荣耀推送服务（HONOR PUSH）是荣耀公司向开发者提供的消息推送服务，通过服务端与客户端建立一条稳定、可靠的长连接通道，向荣耀手机系统（Magic UI）上的APP应用客户端实时推送消息的服务。无论应用进程是否存在，均可正常收到消息。
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。
Jetpack Core	Google	Target the latest platform features and APIs while also supporting older devices.
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。

第三方追踪器检测

名称	类别	网址
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
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
华为HMS Core应用ID的=> "com.huawei.hms.client.appid" : "appid=106014833"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCwzMiwzNSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDM2LDM1LDM0LDMzLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
小米推送的=> "XIAOMI_APPKEY" : "MI-5372016050321"
极光推送的=> "JPUSH_CHANNEL" : "developer-default"
荣耀推送的=> "com.hihonor.push.app_id" : "220711833"

OPPO推送的=> "OPPO_APPID" : "OP-30817665"
OPPO推送的=> "OPPO_APPSECRET" : "OP-f9cee327b01442ac928022d1fb213446"
vivo推送的=> "com.vivo.push.api_key" : "92a088f944e0c9064b35ed3895cca807"
OPPO推送的=> "OPPO_APPKEY" : "OP-a4317e0908fe49e4b28276da3849972e"
小米推送的=> "XIAOMI_APPID" : "MI-2882303761520160321"
极光推送的=> "JPUSH_APPKEY" : "4087612f7cb9f4e2252df2be"
vivo推送的=> "com.vivo.push.app_id" : "105577867"

免责声明及风险提示: