南明离火
移动应用检测平台

ANDROID 静态分析报告

易医文库 • v1.0.0

分析日期: 2024-03-12 08:51:30

应用概览

文件名称:	yywk.app.apk
文件大小:	23.52MB
应用名称:	易医文库
软件包名:	cn.yywkcn
主活动:	cn.yywkcn.MainActivity
版本号:	1.0.0
最小SDK:	19
目标SDK:	30
加固信息:	Flutter/Dart 加固
应用程序安全分数:	48/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	148b4da15239fde421a051e5eee24898
SHA1:	16c858895c0ab31e13441c1c7826d54f3bbec16f
SHA256:	0e152127dab4be82acbc054e309241d3a97d232d5e703669a125746a2826b905

分析结果严重性分布

高危	中危	信息	安全	关注
2	9	2	1	0

四大组件导出状态统计

Activity组件：9个，其中export的有：1个
Service组件：18个，其中export的有：1个
Receiver组件：15个，其中export的有：5个
Provider组件：5个，其中export的有：0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: CN=matx885
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-27 10:06:54+00:00
有效期至: 2092-01-10 10:06:54+00:00
发行人: CN=matx885
序列号: 0x5b745faf
哈希算法: sha256
证书MD5: f1e7d44b3dcf5e853fbdc292de9ea915
证书SHA1: 94a07c3ad1a2584b9a6ebc35a6ebbdef45d467e4
证书SHA256: a2dad851356c00af34f56311ac58a23abcbbb20fe7ab3d5e4af2a6e90f4eeebb
证书SHA512:
83bc24c3e43052dd37b61d7b1700b7969cfcb1f2ef0e5439d85020ed58a2de24f246dc8a77976205b0719521f0955130c2f8c992b5b552f8b7e0283059aaeda

公钥算法: rsa
密钥长度: 2048
指纹: ee7ee40332fca388502d7535dd864c19661e4f76cb9cee1f81976c8bc33918c3
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
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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_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_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.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。
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_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.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.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.VIDEO_CAPTURE	未知	未知权限	来自 android 引用的未知权限。
android.permission.AUDIO_CAPTURE	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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
cn.yywkcn.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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。这也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。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
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.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
cn.yywkcn.MainActivity	Schemes: app.flyweb.scheme://,

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
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就会易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

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有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	警告	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	应用程序数据将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。默认情况下它被设置为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。
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。

5	Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
6	Activity (com.onesignal.NotificationOpenedActivityHMS) 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。
7	Broadcast Receiver (com.onesignal.BootUpReceiver) 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。
8	Broadcast Receiver (com.onesignal.UpgradeReceiver) 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	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
10	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。
11	高优先级的Intent (999) [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: **2** | 警告: **5** | 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
2	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

3	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
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	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
7	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
8	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
9	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
10	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	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	9/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	8/46	com.google.android.c2dm.permission.RECEIVE android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.FLASHLIGHT

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
goo.gl	安全	否	**IP地址:** 142.250.72.174 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
pagead2.googlesyndication.com	安全	否	**IP地址:** 142.250.217.130 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
googlemobileadssdk.page.link	安全	否	**IP地址:** 142.250.72.161 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
flyweb-2020.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

googleads.g.doubleclick.net	安全	否	**IP地址:** 142.250.176.2 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
csi.gstatic.com	安全	否	**IP地址:** 216.239.32.3 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
api.onesignal.com	安全	否	**IP地址:** 104.18.214.59 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
onesignal.com	安全	否	**IP地址:** 104.18.214.59 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://goo.gl/J1sWQy	c/b/b/b/g/i/c.java
• https://onesignal.com/android_frame.html	com/onesignal/h2.java
• https://api.onesignal.com/	com/onesignal/o2.java
• javascript:if(window.flutter_inappwebview	com/pichillilorenzo/flutter_inappwebview/JavaScriptBridgeInterface.java
• http://www.example.com	com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java
• https://github.com/pichillilorenzo/flutter_inappwebview#important-note-for-android • https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects	com/pichillilorenzo/flutter_inappwebview/in_app_webview/FlutterWebView.java
• https://github.com/flutter/flutter/issues/78827	io/flutter/plugin/editing/d.java
• https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/d.java
• https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/k.java

• https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_interstitial.js • https://flyweb-2020.firebaseio.com • https://%s/%s/%s • https://api.onesignal.com/ • https://googlemobileadssdk.page.link/admob-android-update-manifest • https://googlemobileadssdk.page.link/ad-manager-android-update-manifest. • https://firebase.google.com/support/privacy/init-options. • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html • https://github.com/flutter/flutter/issues/2897).It • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html • https://support.google.com/dfp_premium/answer/7160685#push • https://imasdk.googleapis.com/admob/sdkloader/native_video.html • https://plus.google.com/ • https://csi.gstatic.com/csi • https://github.com/flutter/flutter/issues/78827 • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_banner.js • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_expanded_banner.js • https://onesignal.com/android_frame.html • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/native_ads.js • https://googlemobileadssdk.page.link/admob-interstitial-policies • https://developer.android.com/guide/topics/permissions/overview • https://goo.gl/J1sWQy • javascript:if(window.flutter_inappwebview • https://github.com/pichillilorenzo/flutter_inappwebview#important-note-for-android • https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects • https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-app • data:enabled • http://www.example.com	自研引擎分析结果

Firebase 配置安全检测

标题	严重程度	描述信息

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。
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。
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 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。

邮箱地址敏感信息提取

EMAIL	源码文件
u0013android@android.com0 u0013android@android.com	c/b/b/b/d/a0.java
android@android.com0	自研引擎分析结果

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
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://flyweb-2020.firebaseio.com"
"google_api_key" : "AIzaSyDNKy8damDiZfaqCL6uZLBh0UmgluSDHC0"
"google_crash_reporting_api_key" : "AIzaSyDNKy8damDiZfaqCL6uZLBh0UmgluSDHC0"
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
c682b8144a8dd52bc1ad63
5eb5a37e-b458-11e3-ac11-000c2940e62c
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWc2bm9lZ2Vy

免责声明及风险提示: