MoGua

mHealth 3.3.4.APK 分析报告

APP名称: mHealth

包名:	com.moph.mhealth
域名线索:	10条
URL线索:	15条
邮箱线索:	1条
分析日期:	2025年5月27日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: mHealth_3.3.4_APKPure.xapk
文件大小: 11.74MB
MD5值: 85bfeec40c4c71a7adc9b94a8541306b
SHA1值: 3eed4363b90cf8b17fe319c10bb9d59fd84fb035
SHA256值: 59652191bd233afe7960d5ccaa9ca33c85d94e484edf43913b77d3db23219bca

APP 信息

App名称: mHealth
包名: com.moph.mhealth
主活动Activity: com.moph.mhealth.activity.SplashActivity
安卓版本名称: 3.3.4
安卓版本: 269

域名线索

域名	服务器信息
pdf.numedapp.com	**IP**: 157.230.251.92 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
h4u-mhealth.moph.go.th	**IP**: 203.157.103.27 **所属国家**: Thailand **地区**: Nonthaburi

	城市: Bang Bua Thong **纬度**: 13.910200 **经度**: 100.425812
numed-b0fb8.firebaseio.com	**IP**: 35.190.39.113 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
raw.githubusercontent.com	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
numedapp.com	**IP**: 151.101.65.195 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.google.com	**IP**: 157.240.17.35 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
play.google.com	**IP**: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547

health.nux.community	没有服务器地理信息.
moph.go.th	**IP**: 203.157.100.20 **所属国家**: Thailand **地区**: Nonthaburi **城市**: Bang Bua Thong **纬度**: 13.910200 **经度**: 100.425812

URL线索

URL**信息**	Url**所在文件**
https://raw.githubusercontent.com/jaredrummler/AndroidDeviceNames/master/json/devices/%s.json	com/jaredrummler/android/device/DeviceName.java
https://h4u-mhealth.moph.go.th/	com/moph/mhealth/config/ApiClient.java
https://moph.go.th/index.php/mhealth_privacy_notice	com/moph/mhealth/activity/SettingActivity.java
https://h4u-mhealth.moph.go.th/microservice-behavior-mhealth/	com/moph/mhealth/activity/ViewNCDsMenuActivity.java
https://health.nux.community/mhealth/Authorization=	com/moph/mhealth/activity/ViewNCDsMenuActivity.java
https://h4u-mhealth.moph.go.th/h4u-webview/	com/moph/mhealth/activity/MainActivity.java
http://play.google.com/store/apps/details?id=%s&hl=en	com/vansuita/library/CheckNewAppVersion.java
http://www.google.com	com/vansuita/library/CheckNewAppVersion.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://numed-b0fb8.firebaseio.com	摸瓜V1引擎
https://pdf.numedapp.com/TCPDFNUMED/downloadPDF.php?file=	摸瓜V1引擎
https://numedapp.com/user/pdf.html	摸瓜V1引擎
https://numedapp.com/user	摸瓜V1引擎

邮箱线索

邮箱地址	所在文件
assanepoi@gmail.com	com/moph/mhealth/activity/MainActivity.java

手机线索

签名证书

APK已签名

v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2021-06-13 14:55:58+00:00
有效期至: 2051-06-13 14:55:58+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xa5ec7de1ab3e2fd33e1fa2a217c83134cf61a978
哈希算法: sha256
md5值: f554ac0089b8b2aca72362178f5bdd64
sha1值: 4a1c4ef1b370f15601028c7de59b21af0dd71d12
sha256值: a9e52aea76a9eb1326db732c9655562bd87a48c36c70d1ad841415f8062597be
sha512值: 7e94b9eb49b93441b12e84fd7f499135954152ff8535502ad4ec11af4604efc3d0319ba0cdd4caabef40bd614fda0ee28e950abbb1d4c54bc3005d7f4eb000fb
公钥算法: rsa
密钥长度: 4096
指纹: fb9563a90ecf39c5d9298b3fff9186b56a9bae427f9f541244170d90b68f29b8

硬编码敏感信息

可能的敏感信息
"checkEmailOrPassword" : "กรุณาตรวจสอบอีเมล์หรือรหัสผ่าน"
"firebase_database_url" : "https://numed-b0fb8.firebaseio.com"
"google_api_key" : "AIzaSyCkotqL1RVCVdAULNcbTfkX0mEFiLr1gXU"
"google_crash_reporting_api_key" : "AIzaSyCkotqL1RVCVdAULNcbTfkX0mEFiLr1gXU"
"google_maps_key" : "AIzaSyCkotqL1RVCVdAULNcbTfkX0mEFiLr1gXU"
"image_picker_provider_authority_suffix" : ".provider"
"input_header_check_laser_reset_password" : "กรุณายืนยันตัวตนของท่าน เพื่อทำการเปลี่ยนรหัสผ่านใหม่"

"input_header_set_password" : "กรุณาตั้งรหัสผ่าน 6 หลัก"
"input_password" : "ระบุรหัสผ่าน"
"mdtp_deleted_key" : "%1$s deleted"
"password" : "รหัสผ่าน"
"repassword" : "ลืมรหัสผ่าน"
"reset_password" : "รีเซ็ตรหัสผ่าน"
"setting_password" : "แก้ไขรหัสผ่าน"

加壳分析

加壳类型	**所属文件**
登陆摸瓜网站后查看	

第三方插件

名称	**分类**	URL**链接**
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
oppo.permission.OPPO_COMPONENT_SAFE	未知	Unknown permission	Unknown permission from android reference
com.huawei.permission.external_app_settings.USE_COMPONENT	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.USE_FINGERPRINT	正常	allow use of 指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.sec.android.provider.badge.permission.READ	正常	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	正常	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	正常	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	正常	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	正常	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	正常	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	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	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	正常	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	正常	在应用程序上显示通知	在华为手机的应用程序启动图标上显示通知计数或徽章

		计数	
android.permission.READ_APP_BADGE	正常	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	正常	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	正常	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	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。