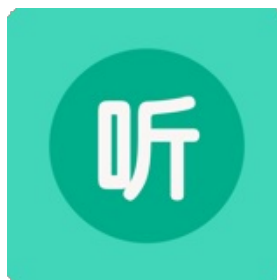




MoGua

昊昊听书 2.62.APK 分析报告



APP名称:

昊昊听书

包名:	com.com.reyou.hh
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2024年5月8日
分析平台:	摸瓜反编译平台

文件名: 昊昊听书 2.62开发版.apk
文件大小: 23.74MB
MD5值: 5447e55d0d8077cd2d39690658a61f52
SHA1值: 0bf9be5ebf494d7363f13737c7128c940db79aa9
SHA256值: 3fe62fab87b51f46381ba43bad94f13fdc899b6f45e554f0b34b3d7d62b1c192

i APP 信息

App名称: 昊昊听书
包名: com.com.reyou.hh
主活动Activity: com.e4a.runtime.android.StartActivity
安卓版本名称: 2.62
安卓版本: 1

🔍 域名线索

域名	服务器信息
crosswalk-project.org	没有服务器地理信息.

🌐 URL线索

URL信息	Url所在文件
https://crosswalk-project.org/).	Mogua Engine V1

✉ 邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: O=coretalk, OU=coretalk, CN=coretalk
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-22 02:54:44+00:00
有效期至: 2047-09-16 02:54:44+00:00
发行人: O=coretalk, OU=coretalk, CN=coretalk
序列号: 0x5bbdde
哈希算法: sha256
md5值: de21ccde40e2e21b8da3da63bff33257
sha1值: 89566fa5ea418c669742ef30d2aa034102257969
sha256值: 72da2312dd5f414e3fa0083bfde6be2fdf5c1f50bdc1923bdeaf629b9f7e70e9
sha512值: f8075349ce19e5d43f936d4bcb10b5c9268ab23f10f9f12b3022d480974ac1729afc304bd5fefdeb592597ee313b37082ea78ce1c24e9c40c4497314a5219cfe
公钥算法: rsa
密钥长度: 2048
指纹: d1361aaa8f8771a9785d8deefec9b4152a94dd8a5ad93ffc08025ceb0a26f7e2

硬编码敏感信息

可能的敏感信息
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"http_auth_title" : "Authentication Required"

"http_auth_user_name" : "Username"
"http_auth_password" : "Password"
"http_auth_log_in" : "Log In"

加壳分析

加壳类型	所属文件
360	libjiagu.so
360	assets/libjiagu.so
360	libjiagu_a64.so
360	libjiagu_x64.so
360	libjiagu_x86.so

第三方SDK

名称	分类	URL链接
360加固	加壳加固, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/456

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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

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_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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等

com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

应用内通信