MoGua

希沃白板 2.1.49.7.53.APK 分析报告

APP名称:	希沃白板

包名:	com.seewo.en
域名线索:	20条
URL线索:	7条
邮箱线索:	1条
分析日期:	2025年7月6日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: EN_Mobile_2.1.49.7.53_normal.apk
文件大小: 132.68MB
MD5值: 811b471687fecc8be6f96214092fb3ab
SHA1值: 0ac78487071f37f3b6e0e0e0f8410d811bfd8d0d
SHA256值: d663a0fa955b943890177c1999300e76f918c10baaf41e1aee2afda94854220b

APP 信息

App名称: 希沃白板
包名: com.seewo.en
主活动Activity: com.seewo.en.activity.VersionFeatureActivity
安卓版本名称: 2.1.49.7.53
安卓版本: 10497

域名线索

域名	服务器信息
grs.dbankcloud.asia	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast'

	城市: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.com	IP: 60.28.200.159 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.eu	没有服务器地理信息.
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
metrics1.data.hicloud.com	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-dra.push.dbankcloud.com	IP: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987

	经度: 103.850281
e.seewo.com	IP: 223.4.221.197 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
data-drru.push.dbankcloud.com	IP: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.platform.dbankcloud.ru	没有服务器地理信息.
easinote.seewo.com	IP: 101.37.44.92 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
data-drcn.push.dbankcloud.com	IP: 121.36.117.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics.dt.dbankcloud.ru	IP: 159.138.204.140 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499

metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
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
argus.agoralab.co	**IP**: 139.215.162.51 **所属国家**: China **地区**: Jilin **城市**: Changchun **纬度**: 43.880001 **经度**: 125.322777
grs.dbankcloud.cn	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

URL线索

URL信息	Url所在文件
https://easinote.seewo.com	摸瓜V1引擎
https://e.seewo.com/download/file?code=SeewoIwbAssistant	摸瓜V1引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics.dt.dbankcloud.ru	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎

https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s	lib/armeabi-v7a/libagora-rtc-sdk.so
http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s	lib/armeabi-v7a/libagora-rtc-sdk.so
https://github.com/opencv/opencv/issues/16739	lib/armeabi-v7a/libda_cropper.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

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: C=CN, ST=GD, L=GZ, OU=CVT
签名算法: rsassa_pkcs1v15

有效期自: 2012-08-28 12:20:26+00:00
有效期至: 2062-08-16 12:20:26+00:00
发行人: C=CN, ST=GD, L=GZ, OU=CVT
序列号: 0x16965713
哈希算法: sha256
md5值: 2fa885a0d1b0a3e5cfb19e8451acef2e
sha1值: 42235e597739d2bbcb173c77564f2d6f2a911c15
sha256值: 799e60235aadee26db1c6b664da38da0f9069cd7059f9cc8a90e001ec0b94f66
sha512值: 30d2c9ec2fc4c2a574c71abe088b5bcbeae9e9db5750efe4898f593bd22b3c814ff85cca7a2d1e2fdf8899f55984ca7ddaed4914e02866578a546bbcb5f0d4ef
公钥算法: rsa
密钥长度: 2048
指纹: daa3fd7df2a5e07c5e3a3b4b05ef0931d4450c679a99c5c32597d7babbeceba9

硬编码敏感信息

可能的敏感信息
"checking_wifi_password" : "正在验证Wifi.."
"courseware_share_copylink_password" : "密码 : %1$s"
"forget_password" : "忘记密码"
"format_login_with_token_of_app" : "使用希沃账号登录%s，点击了解"
"gt_one_login_auth_btn" : "一键登录"
"illegal_password" : "密码只能包含数字，字母和部分特殊字符"
"image_live_not_support_multi_user" : "暂不支持多人拍照上传"
"influence_authentication_score" : "%1$d分"
"influence_rights_authen_desc" : "1. 影响力认证标识，将出现在你的头像处，代表着你对其他老师的影响程度。 2. 标识共分为 4 个等级，分数越高则标识越突出。"

"influence_rights_authentication_value" : "影响力满 %1$d 分，即可获得此权益"
"login_en_token_invalid" : "同一账号已在其它设备登录,非本人操作请尽快 修改密码"
"login_token_invalid" : "登录已过期，请重新登录"
"modify_password" : "修改密码"
"please_retry_auth" : "获取用户信息失败，请重新登录"
"pwd_tip" : " 密码：%1$s"
"reset_password" : "重置密码"
"set_password" : "设置密码"
"store_studio_author" : "创作者： "
"warning_simple_password" : "密码太简单，建议使用8位以上密码"

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.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.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.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.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.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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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.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.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.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

com.seewo.en.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。
com.seewo.en.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.seewo.en.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.seewo.en.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.seewo.en.RouterActivity	Schemes: enmobile://, Hosts: route,
com.tencent.tauth.AuthActivity	Schemes: \ 1106809967://,
