南明离火
移动应用检测平台

ANDROID 静态分析报告

文字转语音精灵 v18

分析日期: 2024-06-02 08:06:51

应用概览

文件名称:	com.smallyin.wenyuelfes_18.apk
文件大小:	46.76MB
应用名称:	文字转语音精灵
软件包名:	com.smallyin.wenyuelfes
主活动:	com.smallyin.wenyuelfes.ui.SplashActivity
版本号:	18
最小SDK:	24
目标SDK:	33
加固信息:	360加固 加固
应用程序安全分数:	49/100 (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:	1afff921881ca1b3f7996f9b7e0ec365
SHA1:	a914ab8b346d39dbac32a24f65c2fcd43968972
SHA256:	d47f6f2d241ddca733c7bc[illegible]001392a4b297172ec7b6e1f23314ea708e233ba1e

分析结果严重性分布

高危	中危	信息	安全	关注
3	18	2	2	9

四大组件导出状态统计

Activity组件：108个，其中export的有： 6个
Service组件：12个，其中export的有： 0个
Receiver组件：2个，其中export的有： 1个
Provider组件：9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: C=wenyuelfes, ST=wenyuelfes, L=wenyuelfes, O=wenyuelfes, OU=wenyuelfes, CN=wenyuelfes
签名算法: rsassa_pkcs1v15
有效期自: 2020-05-12 03:15:41+00:00
有效期至: 2045-05-06 03:15:41+00:00
发行人: C=wenyuelfes, ST=wenyuelfes, L=wenyuelfes, O=wenyuelfes, OU=wenyuelfes, CN=wenyuelfes
序列号: 0x33af7deb
哈希算法: sha256
证书MD5: 2f3e11b4839769851b6d5a9073efaff5
证书SHA1: 4644d63b20fcdd763c9e15434dba3cd63af11b75
证书SHA256: 017223becd7bd6049621cc3a9825854088fc5ffb10d0ae45822d7c2321393637
证书SHA512:
9459133b8ac4f53e0eda28029fa26d6afec71fa3c3de0e5ca92b95995f4abe7bde4b597383adfa5152877e6c21e11e2fb4f3ca3f7b6cf1f0097b25adcde75842

公钥算法: rsa
密钥长度: 2048
指纹: 8a0ff0586888e2234a342e296a8c2f451e86ee12000556c5014cb4d563b52593
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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.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.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.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
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.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。
com.smallyin.wenyuelfes.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
com.smallyin.wenyuelfes.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	Schemes: tencent1106923881://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1		高危	基本配置不安全地配置为允许到所有域的明文流量。

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: **9** | 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 7.0, [minSdk=24]	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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	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。
5	Activity (com.tencent.tauth.AuthActivity) 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。
6	Activity (com.smallyin.wenyuelfes.wxapi.WXEntryActivity) 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。
7	Activity (com.smallyin.wenyuelfes.wxapi.WXPayEntryActivity) 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。
8	Activity (com.alipay.sdk.app.PayResultActivity) 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。
9	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
10	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityProxy) 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。
11	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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。

代码安全漏洞检测

高危: **2** | 警告: **7** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
4	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
5	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
6	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	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
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	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

10	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
11	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
12	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
13	该文件是World Writable。任何应用程序都可以写入文件	高危	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

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/libbdSpilWakeup.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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 warning 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
2	arm64-v8a/libidcard_quality.1.1.1.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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 warning 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

3	arm64-v8a/libidl_license.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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 warning 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
4	arm64-v8a/libocr-sdk.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk']	False warning 符号可用

5	arm64-v8a/libsgcore.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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 warning 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.CAMERA android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	11/46	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS com.google.android.gms.permission.AD_ID

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

www.samsungapps.com	安全	否	**IP地址:** 54.229.93.185 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
www.tingniukeji.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
apps.oceanengine.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.chengzijianzhan.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
aip.baidubce.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 浙江 **城市:** 台州 **纬度:** 28.666668 **经度:** 121.349998 **查看:** 高德地图
www.toutiaopage.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图

mobilegw.alipaydev.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
h5.m.taobao.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874777 **查看:** 高德地图
i.snssdk.com	安全	是	**IP地址:** 49.79.224.209 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://h5.m.taobao.com/mlapp/olist.html	p0/a.java
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
• www.toutiaopage.com/tetris/page • www.chengzijianzhan.com • https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/a.java
• http://tsn.baidu.com/text2audio	com/smallyin/wenyuelfes/net/DownloadUtil.java
• http://www.tingniukeji.com	com/smallyin/wenyuelfes/net/ApiNet.java
• 2.1.1.2	com/byted/live/api/BuildConfig.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• http://tsn.baidu.com/text2audio	com/smallyin/wenyuelfes/ui/SpeechSynthesisActivity.java
• https://loggw-exsdk.alipay.com/loggw/logupload.do	t0/d.java
• https://mcgw.alipay.com/sdklog.do	t0/c.java

• https://ggff2022.oss-cn-beijing.aliyuncs.com/zhifu.txt • https://yinsi2021.oss-cn-beijing.aliyuncs.com/wenziyh.txt • http://www.google.com/ • https://yonghuxieyi2021.oss-cn-beijing.aliyuncs.com/wenziys.txt	com/smallyin/wenyuelfes/ui/AgreementActivity.java
• http://tsn.baidu.com/text2audio	com/smallyin/wenyuelfes/ui/TextPhotoActivity.java
• https://work.weixin.qq.com/kfid/kfcbdf79213c999000c	com/smallyin/wenyuelfes/ui/fragments/PersonFragment.java
• https://mobilegw.alipaydev.com/mgw.htm	x0/k.java
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/ar/wt.java
• https://oss-cn-beijing.aliyuncs.com • https://f-transform.oss-cn-beijing.aliyuncs.com	b2/b.java
• https://mobilegw.alipay.com/mgw.htm	o0/a.java
• https://openapi.baidu.com/oauth/2.0/token?client_id=	s1/a.java
• http://39.98.176.48/niu/aasr/createbyexternal • http://39.98.176.48/niu/aasr/delete • http://www.tingniukeji.com/wenyuelfes/initv3 • http://39.98.176.48/niu/aasr/query • https://aip.baidubce.com/oauth/2.0/token • http://39.98.176.48/niu/acs/getcredentials • http://39.98.176.48/niu/aasr/listpage • http://39.98.176.48/niu/aasr/create	com/smallyin/wenyuelfes/net/ApiManager.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
语音识别 SDK	Baidu	百度语音开放平台 Android SDK，提供短语音识别、实时语音识别、离线自定义命令词识别、远场语音识别、语音合成、语义解析与对话管理等相关接口。SDK内部均为采用流式协议，即用户边说边处理。区别于 Restful 需要上传整个录音文件。
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
RxFFmpeg	microshow	RxFFmpeg 是基于 (FFmpeg 4.0 + X264 + mp3lame + fdk-aac + opencore-amr + openssl) 编译的适用于 Android 平台的音视频编辑、视频剪辑的快速处理框架，包含以下功能：视频拼接，转码，压缩，裁剪，片头片尾，分离音视频，变速，添加静态贴纸和gif动态贴纸，添加字幕，添加滤镜，添加背景音乐，加速减速视频，倒放音视频，音频裁剪，变声，混音，图片合成视频，视频解码图片，抖音首页，视频播放器及支持 OpenSSL https 等主流特色功能。
阿里聚安全	Alibaba	阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。

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。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
快手广告 SDK	快手	快手信息流广告，为您和用户搭建桥梁。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
百度语音识别的=> "com.baidu.speech.API_KEY" : "tAK...FxU0XGWhjid0K2ZO"
百度语音识别的=> "com.baidu.speech.APP_ID" : "19818075"
百度语音识别的=> "com.baidu.speech.SECRET_KEY" : "rIew9UBGaweCjnegdyM6IBABCCUYMau2"
b6cbad6cbd5ed0d209afc69ad6b7dd17efaae9b3c47eabe0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7e6e6e78f15ca98b8ed2eaf86ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649
5bd2d8d1b465156042000ef
e6b1bdc1890370f2f2419fe06d0fdf7628ad0083d52da1ecfe991164711bbf9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c211b4756e1e208775989a4f691bff4bbbc58174d2a96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843df9434b164e0220baabb10c8978c3f4c6b7da79d8220a968356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65fdffd2c080281a6ab20be5879e0330eb7ff70871ce684e7174ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: