南明离火

移动应用检测平台

ANDROID 静态分析报告

Говорим по-английски • v1.13

分析日期: 2025-07-05 13:49:36

应用概览

文件名称:	com.axidep.polyglotenglishreading v1.13.apk
文件大小:	11.12MB
应用名称:	Говорим по-английски
软件包名:	com.axidep.polyglotenglishreading
主活动:	com.axidep.polyglotenglishreading.activities.Main
版本号:	1.13
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	62/100 (低风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	8d2b34bb9a5009bd8d9f6e4b8b9e8308
SHA1:	17f5eda9bf3a1b946f6dd56e358af2507942a3c
SHA256:	de92b3ff4d4d87744f219be45d9e25d419c7145e5289b9c786295f05eeb88b7f

分析结果严重性分布

高危	中危	信息	安全	关注
0	9	2	2	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 0个
Service组件：3个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
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: 2021-10-04 06:59:09+00:00
有效期至: 2051-10-04 06:59:09+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xbe538fede709607e5e8f59ed5bf858b4e9a785d7
哈希算法: sha256
证书MD5: b7d3a65e65a53f15ba40f21acace27f8
证书SHA1: e72e685269840d26daa14c268e491b3e9945dfaa
证书SHA256: e4ae29cacb65ed5fe66f4787f6f7419926b5bc0ede96bc958d615e5be1d75bef
证书SHA512:
6589f7aa71868e71d49188bbc576dfbb65f92736e935d01460f7f66d35e4a24598d2fffd9c7916767520b7563a653e961b42dd0296fc8a[illegible]e11512a73f1fb5ad

公钥算法: rsa
密钥长度: 4096
指纹: 2442a2d9fab7957be76210a4e691bdfe1f545a3a6e969ee8e030bc424b955948
共检测到 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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
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。这样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.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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。
com.axidea.polyglotenglishreading.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用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: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Broadcast Receiver (com.axidep.polyglotenglishreading.BootReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
2	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

本报告由南明离火移动安全分析平台生成

1	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
2	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
3	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
4	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
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限

00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00133	开始录音	录制音视频 命令	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	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	3/30	android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NOTIFICATION_POLICY android.permission.ACCESS_NETWORK_STATE

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
api-project-70698519652.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
words.axidep.ru	安全	否	**IP地址:** 178.253.40.97 **国家:** 俄罗斯联邦 **地区:** 桑克-彼得堡 **城市:** 圣彼得堡 **纬度:** 59.894440 **经度:** 30.264200 **查看:** Google 地图
polyglotmobile.ru	安全	否	**IP地址:** 212.164.71.128 **国家:** 俄罗斯联邦 **地区:** 新西伯利亚州 **城市:** 新西伯利亚 **纬度:** 55.041737 **经度:** 82.934502 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://polyglotmobile.ru	自研引擎-A
• https://github.com/parse-community/parse-server	com/parse/LocalIdManager.java
• https://words.axidep.ru:1338/parse	com/axidep/polyglotenglishreading/Program.java
• https://polyglotmobile.ru/market	d0/f.java
• 8.8.8.8	d0/g.java
• https://accounts.google.com/o/oauth2/revoke?token=	U0/e.java
• https://play.google.com/store/apps/details?id=	X0/C0613b.java
• https://api-project-70698519652.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://api-project-70698519652.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/70698519652/namespaces/firebase:fetch?key=AIzaSyDHE_DUs1FOZRDADQdaxUAp0OEBddi1tGY ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Sign-In	Google	提供使用 Google 登录的 API。
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 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。
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 ProfileInstaller	Google	此库能够提前预填充要由 ART 读取的编译轨迹。

第三方追踪器检测

名称	类别	网址
Bolts	Analytics	https://reports.exodus-privacy.eu.org/trackers/403

敏感凭证泄露检测

可能的密钥
"answerResultSoundKey" : "answerResultSound"
"app_id_for_server_purchases" : "com.axidep.polyglotenglishreading"
"dark_from_key" : "DarkTo"
"dark_to_key" : "DarkFrom"
"firebase_database_url" : "https://api-project-70698519652.firebaseio.com"

"google_api_key" : "AIzaSyDHE_DUs1FOZRDADQdaxUAp0OEBddi1tGY"
"google_app_id" : "1:70698519652:android:cac81b413f73d259552371"
"google_crash_reporting_api_key" : "AIzaSyDHE_DUs1FOZRDADQdaxUAp0OEBddi1tGY"
"startAnswerSoundKey" : "startAnswerSound"
"testSettingsCategoryKey" : "testSettingsCategory"
"voice_settings_engine_key" : "voiceSettingsEngine"
1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM

Google Play 应用市场信息

标题: Полиглот. Говорим по-английски

评分: 4.62 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** com.axidep.polyglotenglishreading

开发者信息: AxiomRun, AxiomRun, None, None, info@axiommobile.ru,

发布日期: 2021年12月27日 **隐私政策:** Privacy link

关于此应用:

不确定你的英语发音？ 每天只需几分钟，您就能正确发音英语单词。 通常那些想要学习正确说话的人很少说话，并且无法从外面听到自己的声音。 您将在应用程序的帮助下纠正这个问题，您将练习英语发音，并且您将能够听到自己的演讲。 教学方法采用内省过程。您可以跟着母语人士重复单词，应用程序会监控正确的发音。 训练阶段： 1. 跟着母语人士重复该单词，查看该单词及其转录。 2. 您可以使用转录作为提示，从屏幕上发音该单词。 3. 您自己发音屏幕上的单词。 在所有阶段，应用程序都会评估您发音的正确性（百分比）。 * 所有课程均由母语人士配音，无需语音合成器 * 跟着母语人士重复英语单词 * 自动识别算法将理解并评估您的语音 * 录制您的演讲并将其与母语人士的演讲进行比较

免责声明及风险提示

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐患。