南明离火
移动应用检测平台

ANDROID 静态分析报告

Dictionary • v6.2.0

分析日期: 2025-03-10 23:48:12

应用概览

文件名称:	Dictionary v6.2.0.apk
文件大小:	44.89MB
应用名称:	Dictionary
软件包名:	eplusmoment.ds.efd
主活动:	eplusmoment.ds.efd.Splash
版本号:	6.2.0
最小SDK:	26
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	f84d03d3012d854ba8fae22bef25b5ba
SHA1:	03a0260d043732216ca3d74a1799ce2bad4220a0
SHA256:	7aa29c2d42e487c9e79f3efe04e797170d7e3936fe884b30b134c6f440bda49

分析结果严重性

高危	中危	信息	安全	关注
1	9	4	1	1

四大组件信息

Activity组件：11个，其中export的有： 1个
Service组件：12个，其中export的有： 1个
Receiver组件：2个，其中export的有： 2个
Provider组件：3个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=Sing Fu Chan
签名算法: rsassa_pkcs1v15
有效期自: 2014-07-03 05:56:53+00:00
有效期至: 2039-06-27 05:56:53+00:00
发行人: CN=Sing Fu Chan
序列号: 0x49c827d
哈希算法: sha256
证书MD5: 4154485afb71de9b54838407beac7057
证书SHA1: ddbf4f8f4f36248ee0736e9ff90d66656de275bd
证书SHA256: 7ef11653e0faa749f3f59ca9e428ee03e4856612c33f7f29875de52a769fa2f8
证书SHA512:
a63a771fa545a03934f0fd82c02aad25f38355b320af52ac2753910a9062e1d44363005a8b407302599e68495af9a9dca5ca5827b198e74336cf4ce2b6a83c4

公钥算法: rsa
密钥长度: 2048
指纹: 9e23e4bafcee93ea1aca201fede9faab870eaa9007f8554041f80cd8eef4062c
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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.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.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。
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。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
eplusmoment.ds.efd.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

本报告由南明离火移动安全分析平台生成

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: 0 | 警告: 4 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	Activity (eplusmoment.ds.efd.Search) 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。
2	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
3	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。
4	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。

安全漏洞检测

高危: 0 | 警告: 4 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置

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	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
3	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
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	SHA-1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	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
7	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

行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	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

00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息
dict-2b79b.firebaseio.com	安全	否	**IP地址:** 94.130.77.194 **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
www.zetetic.net	安全	否	**IP地址:** 94.130.77.194 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
itunes.apple.com	安全	是	**IP地址:** 94.130.77.194 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
x.y	安全	否	No Geolocation information available.
projectlobook.org	安全	否	**IP地址:** 94.130.77.194 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

tatoeba.org	安全	否	**IP地址:** 94.130.77.194 **国家:** 德国 **地区:** 拜仁 **城市:** 纽伦堡 **纬度:** 49.447781 **经度:** 11.068330 **查看:** Google 地图
y.x	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• https://projectlombok.org • https://projectlombok.org/	lombok/eclipse/agent/PatchFixesShadowLoaded.java
• https://projectlombok.org/features/experimental/fieldnameconstants	lombok/eclipse/handlers/HandleFieldNameConstants.java
• https://projectlombok.org	lombok/installer/Installer.java
• https://projectlombok.org/license	lombok/core/Main.java
• https://projectlombok.org/not/calculated	lombok/javac/JavacAST.java
• https://itunes.apple.com/us/app/english-french-dictionary/id859100549?l=zh&ls=1&mt=8 • https://tatoeba.org	eplusmoment/ds/efd/Var.java
• ftp://y.x/b/ • http://x.y/a/	lombok/core/configuration/ConfigurationFile.java
• http://groups.google.com/group/project-lombok	lombok/installer/eclipse/EclipseProductLocation.java
• https://projectlombok.org/not/calculated	lombok/eclipse/EclipseAST.java
• http://play.google.com/store/apps/details?id=	eplusmoment/ds/data/RateUtils.java
• http://play.google.com/store/apps/details?id= • https://itunes.apple.com/us/app/english-french-dictionary/id859100549?l=zh&ls=1&mt=8	eplusmoment/ds/data/ShareUtils.java
• https://translate.google.com/translate_tts?ie=utf-8&q=	eplusmoment/ds/data/TtsManager.java
• https://projectlombok.org/features/experimental/fieldnameconstants	lombok/javac/handlers/HandleFieldNameConstants.java
• https://github.com/sqlcipher/android-database-sqlcipher • https://www.zetetic.net/sqlcipher/ • https://dict-2b79b.firebaseio.com • https://www.zetetic.net/sqlcipher/license/	自研引擎-S

FIREBASE数据库分析

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://dict-2b79b.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/861213595156/namespaces/firebase:fetch?key=AIzaSyDAdUABbgQd9TqVGj0RrILypzSoNQ7ZSmo ） 已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

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 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。
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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	让库能够提前预填充要由 ART 读取的编译轨迹。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱

EMAIL	源码文件
info@eplusmoment.com	eplusmoment/ds/data/ContactUtils.java

追踪器

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

密钥凭证

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-7842774101690929~5294789493"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://dict-2b79b.firebaseio.com"
"google_api_key" : "AIzaSyDAdUABbgQd9TqVGj0RrILypzSoNQ7ZSmo"
"google_app_id" : "1:861213595156:android:bc0e7c8c09ec7988a63901"
"google_crash_reporting_api_key" : "AIzaSyDAdUABbgQd9TqVGj0RrILypzSoNQ7ZSmo"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
BBCD3226BBD92D4C90E7690BBBC04369
123450781234aa7812345
C95A010E0A27A283CC9F3F82C70A2D37

GooglePlay应用信息

标题: French English Dictionary

评分: 4.352941 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 教育 **Play Store URL:** eplusmoment.ds.efd

开发者信息: EPlusMoment, EPlusMoment, None, http://www.eplusmoment.com, eplusmoment@gmail.com,

发布日期: 2014年7月30日 **隐私政策:** Privacy link

关于此应用:

法语英语词典是一种高品质和人性化的词典可在手机和平板。而且它是免费的！它会给你带来一个很好的和愉快的学习经验！ 词典功能： □人性化设计 □通过英语或法语搜索 □快速搜索技术 □大型数据库的单词和短语 □正宗英语/法语发音 □离线搜索 □复制搜索结果 □收藏功能，用于存储单词 □历史功能，用于召回的搜索记录 □通过Facebook，Twitter，WhatsApp的，行等分享结果... 在字典中，您可以搜索并在两个方向，即英语翻译成法语或法语到英语。以上翻译，你可以学会说话的正确语法两种语言的短语或词汇。这个程序是最好的语言更精简，初学者和孩子们，把应用程序与你，你是有经验或课程时。 这个翻译提供翻译地道的发音。你可以听到在字典中的声音和音频。因此，说话和说短语和词汇在不同的行话。搜索功能脱机工作完全没有互联网连接。这种语言使能器/转换器绝对是你所需要的旅游，商务和学习在法国

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端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隐患。