南明离火
移动应用检测平台

ANDROID 静态分析报告

Tagalog - English Translator •
v1.7.7

分析日期: 2025-10-10 21:32:15

应用概览

文件名称:	2ec6790b0d2c56e600ad1bd1ee3447e6d21ae15ad05606c0237cec32c55262f3.apk
文件大小:	7.86MB
应用名称:	Tagalog - English Translator
软件包名:	net.fileden.translator
主活动:	net.fileden.translator.activities.SplashActivity
版本号:	1.7.7
最小SDK:	23
目标SDK:	36
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	58/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	d04a027201bbc9feb1ca50518dd04f00
SHA1:	1f9daa7821d5c319c58757b8eff614aa632080cc
SHA256:	2ec6790b0d2c56e600ad1bd1ee3447e6d21ae15ad05606c0237cec32c55262f3

分析结果严重性分布

高危	中危	信息	安全	关注
1	14	3	3	0

四大组件导出状态统计

Activity组件：11个，其中export的有： 1个
Service组件：10个，其中export的有： 1个
Receiver组件：11个，其中export的有： 2个
Provider组件：4个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
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: 2018-04-30 05:23:46+00:00
有效期至: 2048-04-30 05:23:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x5bd5c479a1ed9e5c9358a3c676567fbb12b203de
哈希算法: sha256
证书MD5: 1024e5d1a2c95cdf08945c58f940b874
证书SHA1: 9a90f09212a9d973cefbc0f2789cf1a3961ab0fb
证书SHA256: dbdde25dd03b42c3a5bb6e77cfac840e39ca6283e1d22acab6711247bea12479
证书SHA512:
34c0398b2097ca0420e676dfe721027d1f464fcb332eaa7aa19f5dd75934cfb5ad603a8a1649223d19a0f97ebb4b0a66cb295e931e331f47f59efda1f39c82f4

公钥算法: rsa
密钥长度: 4096
指纹: 6e6ed791593fc0bf8fd1c2ec3d4e3347f9f20b5347e738b4a9bf7d84d6911145
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.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.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.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。
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.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.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。
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）
net.fileden.translator.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

com.android.vending.CHECK_LICENSE	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: **1** | 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: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F160006]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
4	Activity (net.fileden.translator.activities.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

7	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: **6** | 信息: **3** | 安全: **2** | 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	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	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
5	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
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

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	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
10	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
11	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
00034	查询当前数据网络类型	信息收集 网络	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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
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
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
00014	将文件读入流并将其放入 JSON 对象中	文件	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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	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
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
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
00003	将压缩后的位图数据放入JSON对象中	相机	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
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	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	1/30	android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
pagead2.googlesyndication.com	安全	是	**IP地址:** 220.181.174.166 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
goo.gle	安全	否	**IP地址:** 67.199.248.13 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图

admob-app-id-4619182120.firebaseio.com	安全	否	**IP地址:** 220.181.174.97 **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
app-measurement.com	安全	是	**IP地址:** 220.181.174.97 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.40739 **查看:** 高德地图
youtrack.jetbrains.com	安全	否	**IP地址:** 3.33.8[illegible].220 **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
fileden.net	安全	否	**IP地址:** 172.67.131.78 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.72.238 **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

URL 链接安全分析

URL信息	源码文件
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	D1/c.java
• https://app-measurement.com/a • https://app-measurement.com/s/d	s2/AbstractC2543D.java
• www.google.com	F1/m.java
• https://play.google.com/store/apps/dev?id=6463477096470941816	l3/c.java
• https://plus.google.com/	c2/L.java
• https://fileden.net/privacy.html	a5/c.java
• https://firebase.google.com/support/privacy/init-options	G3/d.java

• https://goo.gl/naoooi	s2/l1.java
• https://youtrack.jetbrains.com/issue/kt-55980	p4/k.java
• https://fundingchoicesmessages.google.com/a/consent	o2/C2347b.java
• https://goo.gle/admob-android-update-manifest • https://goo.gle/ad-manager-android-update-manifest	G1/N0.java
• https://admob-app-id-4619182120.firebaseio.com • https://play.google.com/store/apps/details?id=net.fileden.translator	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase数据库未授权访问	危险	位于 https://admob-app-id-4619182120.firebaseio.com/.json 的 Firebase 数据库在没有任何身份验证的情况下暴露在互联网上。响应内容如下所示：
		
		{
		"2DfjkeJxHJTkdhz5VNVwFJzAeuD": {
		"id": "insecure-firebase-database"
		},
		"poc": {
		"aa977e7f938a3d84e8ec771a9729ca5": "4d5c3579b75a63cbae0f84f4c6e5df6e765f199"
		},
		"test": {
		"-OJ3mL1XxmZWXDN6pLPk": {
		"email": "mr-k0anti@wearehackerone.com",
		"message": "this firebase has been found unprotected by mr-k0anti",
		"username": "mr-k0anti"
		}
		},
		"version": 15
		}

Firebase远程配置已禁用	安全	Firebase远程配置URL（https://firebaseremoteconfig.googleapis.com/v1/projects/720084257006/namespaces/firebase:fetch?key=AIzaSyAN8QLzgH9dpZDdHQGATyfPq6N65krVhYc ）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 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。
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。
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 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。

邮箱地址敏感信息提取

EMAIL	源码文件
pakat.apps@gmail.com	U2/ViewOnClickListenerC0174a.java

第三方追踪器检测

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

敏感凭证泄露检测

可能的密钥
AdMob广告平台的："com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-6737922485518267~8364732180"
"app_id" : "ca-app-pub-6737922485518267~8364732180"
"com.google.firebase.crashlytics.mapping_file_id" : "f7559ce568054b168a27f3cbb8c63694"
"firebase_database_url" : "https://admob-app-id-4619182120.firebaseio.com"
"google_api_key" : "AIzaSyAN8QLzgH9dpZDdHQGATyfPq6N65krVhYc"
"google_app_id" : "1:720084257006:android:2a1573554792df73"
"google_crashlytics_reporting_api_key" : "AIzaSyAN8QLzgH9dpZDdHQGATyfPq6N65krVhYc"
"key_clear_bookmark" : "clear_bookmark"

"key_clear_history" : "clear_history"
"key_disclaimer" : "key_disclaimer"
"key_feedback" : "key_feedback"
"key_font_size" : "key_font_size"
"key_font_typeface" : "key_font_typeface"
"key_privacy" : "key_privacy"
"key_version" : "key_version"
VVZWc05sbFdUalZSVkZveVkxUkNXVlpVVmpOWFJXUldVMFJHYUdFd09YbGxiV1JHVXpKa2NsSjZVbk5rUkVwUVRVaFdTZz09
c103703e120ae8cc73c9248622f3cd1e
B3EEABB8EE11C2BE770B684D95219ECB
AbstractViewOnTouchListenerC2436v0
WVVoU01HTklUVFpNZVRsdFlWZDRiRnBlVm5WTWJUVnNaRU01YUdOSVFucE1Na1pyWWxkc2RVd3lSbmRoVXpnOQ==
470fa2b4ae81cd56ecbcda9735803434cec591fa

Google Play 应用市场信息

标题: Filipino-English Translator

评分: 4.416268 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 图书与工具书 **Play Store URL:** net.fineden.translator

开发者信息: Pakat Apps, 6463477096470941816, None, http://fineden.net, pakat.apps@gmail.com,

发布日期: 2018年7月31日 **隐私政策:** Privacy link

关于此应用:

快速轻松地在菲律宾语（他加禄语）和英语之间进行翻译。这款应用不仅可以翻译单词和句子，还会在可用时显示词典定义——使其成为语言学习者、旅行者和日常使用的实用工具。 功能： • 界面简洁，易于使用 • 菲律宾语翻译成英语和英语翻译成他加禄语 • 翻译单个单词或整句 • 词典定义可用时显示 • 支持明暗主题（根据系统设置） • 从剪贴板粘贴文本即可快速翻译 • 直接从其他应用翻译共享的文本 • 为单词或句子添加书签以备将来参考 • 随时查看翻译历史记录 注意事项： • 翻译需要互联网连接 • 使用特殊字符或不受支持的字符可能会导致应用崩溃 免责声明： 翻译和定义由 Google Cloud Translation API 提供支持。准确性可能会有所不同。开发者对因使用此应用而导致的任何错误、遗漏或后果概不负责。

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。