



ANDROID 静态分析报告



Translator Pro 1.0

分析日期: 2024-08-01 14:01:34

i应用概览

文件名称:	Translator Pro.apk
文件大小:	5.28MB
应用名称:	Translator Pro
软件包名:	com.translation
主活动:	.MainActivity
版本号:	1.0
最小SDK:	12
目标SDK:	32
加固信息:	未加壳
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	2 个杀毒软件报毒
MD5:	d4b911ca6de3a0309d2da6158f95e9bb
SHA1:	829ec4e36316c21bf52a02a495a1b444cb0821f5
SHA256:	991ab0ac70659dc59532f85d904badc247113fa55c707a87520657c2a6b39fcf

📊分析结果严重性分布

🔴 高危	🟡 中危	🟢 信息	✅ 安全	🔍 关注
1	3	2	0	1

📦四大组件导出状态统计

Activity组件: 9个, 其中export的有: 0个
Service组件: 0个, 其中export的有: 0个
Receiver组件: 0个, 其中export的有: 0个
Provider组件: 0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: CN=Lovely, OU=Lovely, O=Lovely, L=Abeokuta, ST=Ogun State, C=NG
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-14 10:05:35+00:00
有效期至: 2123-07-14 10:05:35+00:00
发行人: CN=Lovely, OU=Lovely, O=Lovely, L=Abeokuta, ST=Ogun State, C=NG
序列号: 0x190b0b49444
哈希算法: sha512
证书MD5: 466290a4156fa5b7619ecff1c519d793
证书SHA1: cb34c644f49acb6e7bc6819e303cb710a1bb9ead
证书SHA256: 29ad6877dd9e1f90296d88540092a54c098ecc6d28ca131d5c41ac0644b9963d
证书SHA512:
d0a7e8a4dfbeca1da5a4b5267e07beb178103d7375c677ff1046d686cae73355fc40d7f60329c72021c2de6cf86786d47043e103712c66206f9ce4e3e46502fa

公钥算法: rsa
密钥长度: 2048
指纹: 929f1fabaa432bd8f5f68fd2210bf73cf4d8918adaf43c1f6cd9af942f8cbefe
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.ACCESS_NETWORK_CONDITIONS	未知	未知权限	来自 android 引用的未知权限。
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.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。

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: 2 | 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 3.1, [minSdk=12]	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。

</> 代码安全漏洞检测

高危: 1 | 警告: 6 | 信息: 2 | 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-5	升级会员: 解锁高级权限
2	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
3	SHA-1是已知存在碰撞冲突的弱哈希	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
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	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

6	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
7	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
8	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
9	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	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	2/30	android.permission.RECORD_AUDIO android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_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
----	----	------	------

config.unityads.unitychina.cn	安全	是	IP地址: 116.207.185.33 国家: 中国 地区: 湖北 城市: 宜昌 纬度: 30.714531 经度: 111.283882 查看: 高德地图
config.unityads.unity3d.com	安全	否	IP地址: 34.110.229.214 国家: 美利坚合众国 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

🌐 URL 链接安全分析

URL信息	源码文件
- https://config.unityads.unitychina.cn/webview/ - https://config.unityads.unity3d.com/webview/	com/unity3d/services/core/properties/SdkProperties.java
javascript:window.nativebridge.receiveevent	com/unity3d/services/ads/webplayer/WebPlayerView.java
- https://config.unityads.unity3d.com/webview/ - https://config.unityads.unitychina.cn/webview/ 127.0.0.1 - javascript:window.nativebridge.receiveevent	自研引擎-S

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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。

🕵️ 第三方追踪器检测

名称	类别	网址
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成