南明离火
移动应用检测平台

ANDROID 静态分析报告

天天泰语 • v22.03.07

分析日期: 2024-08-15 16:09:53

应用概览

文件名称:	202203071729440btya.apk
文件大小:	13.49MB
应用名称:	天天泰语
软件包名:	com.yunchuan.thai
主活动:	com.yunchuan.thai.SplashActivity
版本号:	22.03.07
最小SDK:	21
目标SDK:	30
加固信息:	360加固 加固
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	2/432
杀软检测:	5 个杀毒软件报毒
MD5:	6c5adb2d4cb8504e03f2f5de0646b793
SHA1:	608383e30b632853dfb022ff9[illegible]3d4defafc84182
SHA256:	9dcbb794e2c3471fcda185[illegible]f073c8ad41fecb2a87[illegible]960b61b68ec1149320

分析结果严重性分布

高危	中危	信息	安全	关注
1	10	2	1	1

四大组件导出状态统计

Activity组件：21个，其中export的有： 4个
Service组件：2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: True
v4 签名: False
主题: CN=YeChen
签名算法: rsassa_pkcs1v15
有效期自: 2020-09-02 03:46:07+00:00
有效期至: 2045-08-27 03:46:07+00:00
发行人: CN=YeChen
序列号: 0x38b083bd
哈希算法: sha256
证书MD5: 1f46516e7742bd62ecc37ab1deb748a4
证书SHA1: 6d98da568fd301db3724011851b171fdc8f5352d
证书SHA256: 0cac60e9706f7215a814057187b57346f4d734477c524d0c61592d2253e03162
证书SHA512:
b09e4c967542f587d47d851186ae3ff77ded6858efbdceef3f54af6e6876fe81908ccd92e63671e65fd3b3aed9cdce0c91ae9488174ae4e18c34f2a23bfe9ad23

公钥算法: rsa
密钥长度: 2048
指纹: 87ab7344ef69b5d6259043ad043bb657915e67b2510185e920f64d7f00fc0fc1
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.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.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.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。
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.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.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。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

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: **7** | 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 5.0-5.0.2, [minSdk=21]	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设置了TaskAffinity属性 (com.yunchuan.thai.wxapi.WXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
6	Activity (com.yunchuan.thai.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.yunchuan.thai.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。

代码安全漏洞检测

高危: **0** | 警告: **7** | 信息: **2** | 安全: **1** | 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	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

10	MD5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

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.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS

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
app.yunchuan.info	安全	是	**IP地址:** 47.113.102.126 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://app.yunchuan.info	com/yunchuan/mylibrary/BuildConfig.java
• www.baidu.com	com/yunchuan/mylibrary/net/util/NetWorkUtil.java
• https://more-app.oss-cn-beijing.aliyuncs.com/泰语/	com/yunchuan/thai/util/Constant.java
• http://api.fanyi.baidu.com/api/trans/vip/translate?appid=20210115000672160&q=	com/yunchuan/thai/ui/translate/TranslateFragment.java

• http://app.yunchuan.info	com/yunchuan/mylibrary/net/RetrofitServiceManager.java
• https://more-app.oss-cn-beijing.aliyuncs.com/泰语/中级对话/ • https://more-app.oss-cn-beijing.aliyuncs.com/泰语/中级对话素材/	com/yunchuan/thai/ui/SessionDetailActivity.java
• http://yuyin.baidu.com/docs/tts/122	com/yunchuan/thai/util/tts/TTSUtils.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
离线语音合成 SDK	Baidu	百度语音开放平台。纯离线语音合成 SDK 可直接在设备终端进行语音合成，首次使用需要联网，其余时间均可以使用离线合成，为您提供稳定一致、流畅自然的合成体验。
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。
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。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司海量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
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 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。

第三方追踪器检测

名称	类别	网址
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
60c31b0ae04[redacted]1df91
fa942052[redacted]baae229aae75468eb77
b862f9616892871d646faf301108c4bb
5eb3cd2fdbc2ec0771f15576

免责声明及风险提示: