南明离火
移动应用检测平台

ANDROID 静态分析报告

PoChat • v1.0

分析日期: 2024-08-02 12:36:47

应用概览

文件名称:	pochat11.0.apk
文件大小:	1.8MB
应用名称:	PoChat
软件包名:	cn.pochat.new
主活动:	com.e4a.runtime.android.StartActivity
版本号:	11.0
最小SDK:	21
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	1/432
杀软检测:	13 个杀毒软件报毒
MD5:	34b974fd38307eefa438b96d8102c79f
SHA1:	78b05caacc4b9f573059b58[illegible]0816a6a20e8
SHA256:	9ff91f44b9e3e990c284ff[illegible]9db5af9494c5fb3cfd1f[illegible]5ae4f0d6c0f54018f

分析结果严重性分布

高危	中危	信息	安全	关注
1	4	0	0	3

四大组件导出状态统计

Activity组件：2个，其中export的有：1个
Service组件：0个，其中export的有：0个
Receiver组件：1个，其中export的有：0个
Provider组件：1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: False
v3 签名: False
v4 签名: False
主题: C=网页转应用, ST=网页转应用, L=网页转应用, O=网页转应用, OU=网页转应用, CN=网页转应用
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-03 07:43:54+00:00
有效期至: 5022-05-07 07:43:54+00:00
发行人: C=网页转应用, ST=网页转应用, L=网页转应用, O=网页转应用, OU=网页转应用, CN=网页转应用
序列号: 0x707321d8
哈希算法: sha512
证书MD5: 9e5490ee124db602ad2d8a779b009eb9
证书SHA1: 0893164663e47eb9584f3723fb650d5afdfa6efe
证书SHA256: ab86d5d4548c735eda2f8b49fd4fcda1a65b963fb00f8069d73b71b876e87419
证书SHA512:
138aed959a1358134160264d5b102ec24fc5a7de4fd9cf073316c83f04c5d2b4a1a82fc6087a51ce6ca8df3cd262582f37e81ba3824...8e5251e0c4f245541cb9

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
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
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）
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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_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.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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.INSTALL_SHORTCUT	普通	允许在启动器中安装快捷方式	允许应用程序在Launcher中安装快捷方式。
android.permission.UNINSTALL_SHORTCUT	普通	删除快捷方式	允许应用程序删除快捷方式。不再支持此权限。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android 11新增权限，读取本地文件，如简历，聊天图片。

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: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

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 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	Activity (com.e4a.runtime.android.mainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

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
www.123[illegible].com	安全	是	**IP地址:** 58.220.65.19 **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

bbs.e4asoft.com	安全	是	**IP地址:** 43.248.189.45 **国家:** 中国 **地区:** 江苏 **城市:** 宿迁 **纬度:** 33.933334 **经度:** 118.283333 **查看:** 高德地图
ulogs.umengcloud.com	安全	是	**IP地址:** 58.220.65.19 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.77799 **查看:** 高德地图
bbs.e4asoft.compath	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://sc.t1i.cc/function/update/Android/nversion/2.0/	自研引擎-A
• http://bbs.e4asoft.com;path=/ • http://bbs.e4asoft.com/openapi_unsafe.php • https://ulogs.umengcloud.com • http://api.fanyi.baidu.com/api/trans/vip/translate?q= • 10.0.0.172 • http://www.123cha.com/	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
64d4be9ca1a164591b67e2cc

本报告由南明离火移动安全分析平台生成

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。