南明离火
移动应用检测平台

ANDROID 静态分析报告

欲漫涩 • v4.0.3

分析日期: 2024-02-26 14:04:29

应用概览

文件名称:	cartoon240225_cartoon_240202_4.0.3 113.apk
文件大小:	41.71MB
应用名称:	欲漫涩
软件包名:	com.md.cartoon240225
主活动:	com.example.cartoonclient.MainActivity
版本号:	4.0.3
最小SDK:	21
目标SDK:	29
加固信息:	Flutter/Dart 加固
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：可能有安全隐患
MD5:	58f992ffbc1d727f985924028ce11bec
SHA1:	a258d07547faff2c8a812240d4e5806c293a4967
SHA256:	26d14b1857483a96a8dcc84fea6a82893c3bfaf722e2e9cb352389efe7d06cf

分析结果严重性分布

高危	中危	信息	安全	关注
2	1	2	1	0

四大组件导出状态统计

Activity组件：16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：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: True
v3 签名: False
v4 签名: False
主题: C=cartoon240225, ST=cartoon240225, L=cartoon240225, O=cartoon240225, OU=cartoon240225, CN=cartoon240225
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-23 02:35:35+00:00
有效期至: 2051-07-11 02:35:35+00:00
发行人: C=cartoon240225, ST=cartoon240225, L=cartoon240225, O=cartoon240225, OU=cartoon240225, CN=cartoon240225
序列号: 0x4e0a53e6
哈希算法: sha256
证书MD5: a8c9cb3f9a99d1331f70651c45c81525
证书SHA1: 6816b500fe0df37921a45409021ba6cc9db78897
证书SHA256: 0283fc4a95ef3599313992f64211547a668d57f3c1a02513ff600debc0b2ae51
证书SHA512:
0dc9f171fd19f150241a1146e202d3ca41aa7cc49da7a78086cb7294fd8279f1c14da49eb23284a5bbc9f0651df101c6c07921aad2b1f68aad4240a9a148db1

公钥算法: rsa
密钥长度: 2048
指纹: 2fe84bc61fab6ca39a77ffecae935307d7469cf5d45650a32846358801a72bee
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.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.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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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_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.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。
android.permission.READ_PRIVILEGED_PHONE_STATE	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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	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]	警告	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	应用程序具有网络安全配置 [android:networkSecurityConfig=0x7f110003]	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。
3	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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: **2** | 警告: **6** | 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	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
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	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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
7	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
8	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
9	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	警告	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
10	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
11	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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	6/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE
其它常用权限	5/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_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
api2.amplitude.com	安全	否	**IP地址:** 35.81.230.58 **国家:** United States of America **地区:** Oregon **城市:** Portland **纬度:** 45.523449 **经度:** -122.676208 **查看:** Google 地图
dashif.org	安全	否	**IP地址:** 185.199.108.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
exoplayer.dev	安全	否	**IP地址:** 185.199.111.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
regionconfig.amplitude.com	安全	否	**IP地址:** 108.156.91.98 **国家:** United States of America **地区:** Illinois **城市:** Chicago **纬度:** 41.875744 **经度:** -87.618889 **查看:** Google 地图
schemas.microsoft.com	安全	否	**IP地址:** 13.107.253.49 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图

aomedia.org	安全	否	**IP地址:** 185.199.108.153 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
stackoverflow.com	安全	否	**IP地址:** 104.18.32.7 **国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.80667 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://regionconfig.amplitude.com/ • https://api2.amplitude.com/	com/amplitude/api/Constants.java
• data:image	com/bumptech/glide/load/model/DataUrlLoader.java
• file:///	com/luck/picture/lib/widget/longimage/ImageSource.java
• file:///	com/luck/picture/lib/widget/longimage/SubsamplingScaleImageView.java
• https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
• https://github.com/flutter/flutter/issues/29907)	io/flutter/plugin/platform/PlatformViewsController.java
• https://developer.android.com/reference/javax/net/ssl/SSLSocket	io/flutter/plugins/videoplayer/VideoPlayerPlugin.java
• https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects	io/flutter/view/FlutterView.java

• file:/// • http://ns.adobe.com/xap/1.0/ • data:cs:AudioPurposeCS:2007 • https://aomedia.org/emsg/ID3 • https://stackoverflow.com/q/5189914/28465 • http://dashif.org/guidelines/last-segment-number • https://api2.amplitude.com/ • http://dashif.org/guidelines/trickmode • data:image • https://developer.apple.com/streaming/emsg-id3 • https://regionconfig.amplitude.com/ • http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense • https://groups.google.com/d/msg/guava-announce/zHZTFg7YF3o/rQNnwdHeEwAJ • https://exoplayer.dev/issues/player-accessed-on-wrong-thread	自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方跟踪器检测

名称	类别	网址
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125

敏感凭证泄露检测

可能的密钥
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

免责声明及风险提示: