ANDROID 静态分析报告

笔趣阁完美版 • v7.7.5

分析日期: 2024-03-29 09:16:22

应用概览

文件名称:	biqugewmb_2.7.5_7273.com.apk
文件大小:	32.21MB
应用名称:	笔趣阁完美版
软件包名:	com.bqgxyxs.wgg
主活动:	io.legado.app.xnovel.work.NovelWelcomeActivity
版本号:	2.7.5
最小SDK:	21
目标SDK:	32
加固信息:	360加固 加固
应用程序安全分数:	51/100 (中风险)
杀软检测:	4 个杀毒软件报毒
MD5:	cd2487bcecf602c3cf19b11f699905b9
SHA1:	40640bf2741c6f1cfd960e7817947789abbebd4f
SHA256:	83cb25be9829501e107a3b42[illegible]203fdabe3f12ea4[illegible]377c0e31e2af

分析结果严重性分布

高危	中危	信息	安全	关注
1	14	10	1	2

四大组件导出状态统计

Activity组件：94个，其中export的有：6个
Service组件：23个，其中export的有：1个
Receiver组件：4个，其中export的有：2个
Provider组件：10个，其中export的有：1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: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704dc9bb3711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.ACCESS_WIFI_STATE	普通	查看WLAN状态	允许应用程序查看有关Wi-Fi状态的信息。
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.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.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.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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。

android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.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.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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。

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
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: **12** | 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=@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。
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。
4	Activity (io.legado.app.ui.book.read.ReadBookActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
5	Activity (io.legado.app.ui.book.read.pure.PureReadBookActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
6	Service (io.legado.app.service.WebTileService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
7	Broadcast Receiver (io.legado.app.receiver.MediaButtonReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
8	Content Provider (io.legado.app.api.ReaderProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
9	Activity (com.canhub.cropper.CropImageActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
10	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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，因此使其对设备上的任何其他应用程序都可访问。

本报告由南明离火移动安全分析平台生成

12	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
13	Broadcast Receiver (com.taobao.accs.EventReceiver) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED（裁剪符号表）

1	arm64-v8a/libtnet-3.1.14.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.CAMERA android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	10/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_NOTIFICATION_POLICY android.permission.FLASHLIGHT 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

www.coolapk.com	安全	是	**IP地址:** 58.215.114.233 **国家:** China **地区:** Jiangsu **城市:** Wuxi **纬度:** 31.568871 **经度:** 120.288567 **查看:** 高德地图
alanskycn.gitee.io	安全	是	**IP地址:** 180.76.198.77 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** United Kingdom of Great Britain and Northern Ireland **地区:** England **城市:** Warrington **纬度:** 52.184460 **经度:** -0.687590 **查看:** Google 地图
discord.gg	安全	否	**IP地址:** 162.159.130.234 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
gedoor.github.io	安全	否	**IP地址:** 185.199.109.153 **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

URL 链接安全分析

URL信息	源码文件

- https://m.qidian.com/book/1015609210
- http://www.vinterwebb.se/
- http://tts.baidu.com/text2audio
- https://www.beta.browxy.com
- https://goo.gl/2aRDsh
- https://pan.miaogongzi.net
- https://www.zaixianai.cn/voice/
- https://www.yuque.com/legado
- https://github.com/tumuyan
- https://cdn.jsdelivr.net/gh/gedoor/gedoor.github.io
- https://www.yooread.net/e/search/
- http://code.google.com/p/swfobject/
- https://github.com/celetor/web-yuedu3
- https://goo.gl/S9QRab
- https://regexr.com
- https://alanskycn.gitee.io/teachme/assets/font/Source
- https://www.jianguoyun.com/d/home
- https://www.yooread.net/e/search/index.php
- https://cdn.jsdelivr.net/gh/Celeter/build/.github/scripts/speaker.json
- https://goo.gl/nhQhGp
- http://profandesign.se/swfupload/
- https://Cloud.miaogongzi.net/images/icon.png
- https://alanskycn.gitee.io/teachme/Rule/source.html
- https://www.w3cschool.cn/regex_rmjc
- https://www.zaixianai.cn/voiceCompose
- https://alanskycn.gitee.io/teachme/Rule/rss.html
- https://github.com/gedoor/legado/blob/master/app/src/main/java/io/legado/app/help/JsExtensions.kt
- http://tool.uis.cc/jsmin/
- https://zhuanlan.zhihu.com/p/29436838
- https://ai.aliyun.com/nls/tts
- http://www.opensource.org/licenses/mit-license.php
- https://github.com/h11128
- http://mmbiz.qpic.cn/mmbiz_png/hpfMV8hEuL2eS6vnCxvTzoGIa...AibY6exBzJWq9xMic9xDg...Yx...ick87tsfafic0icRwkQ5ibV0bJ84JtSuxhPuEDVquA/0?wx_fmt=png
- https://github.com/Celeter
- http://www.swfupload.org
- https://www.zhaishuyuan.com/chapter/30394/20...
- https://www.jianshu.com/p/3c471953e36d
- https://github.com/AndyBernie
- http://baidu.com
- https://www.jianguoyun.com/d/sign...
- https://zhuanlan.zhihu.com/p/32...
- http://ku.mumuceo.com/static/images/applogo/yuedu.png
- https://cdn.jsdelivr.net/gh/Celeter/build/.github/scripts/ttsDemo.js
- https://github.com/zsakvo
- https://alanskycn.gitee.io/teachme
- https://www.qidian.com
- https://www.zaixianai.cn/Api_getVoice
- https://www.zhaishuyuan.com/read/30394
- http://jquery.org/license
- http://sizzlejs.com/
- https://github.com/gedoor/legado
- https://www.baidu.com
- https://www.qidian.com/rank/yuepiao?page=
- http://www.alistapart.com/articles/flashsatay
- https://github.com/dacer
- https://dav.jianguoyun.com/dav/
- https://www.lanzoux.com/ibjBspkn05i
- http://swfupload.googlecode.com
- http://tts.baidu.com/text2audio
- https://github.com/litcc

自研引擎分析结果

• https://github.com/gedoor/legado/releases/latest • https://discord.gg/qde52p5xgw • https://t.me/legado_channels • https://gedoor.github.io/mybookshelf/ • https://github.com/gedoor/legado • https://www.coolapk.com/apk/256030 • https://alanskycn.gitee.io/teachme/ • http://%1$s:%2$d • https://github.com/gedoor/legado/graphs/contributors	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
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。
C++ 共享库	Android	在 Android 应用中运行原生代码。
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实时监控平台，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。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
烈焰弹幕使	Bilibili	烈焰弹幕使是 Android 上开源的弹幕解析绘制引擎项目
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，找到产品迭代方向，实现精细化运营，全面提升业务增长效能。

敏感凭证泄露检测

可能的密钥
友盟统计的 "UMENG_CHANNEL" : "baidu3_2"
友盟统计的 "UMENG_APPKEY" : "6[illegible]41c92a517ed710[illegible]4f5a"
"custom_page_key" : "自定义翻页按键"
"next_page_key" : "下一页按键"
"volume_key_page_on_play" : "朗读时音量键翻页"
"prev_page_key" : "上一页按键"
"search_book_key" : "搜索书名、作者"
"page_key_set_help" : "将焦点放到输入框按下物理按键会自动录入键值,多个按键会自动用英文逗号隔开."
"author" : "作者"
"author" : "Author"

本报告由南明离火移动安全分析平台生成

"checkAuthor" : "校验作者"
"volume_key_page" : "音量键翻页"
"r_author" : "作者规则(author)"

免责声明及风险提示: