南明离火
移动应用检测平台

ANDROID 静态分析报告

冬瓜音乐 • v1.0.7

分析日期: 2025-10-07 22:34:49

应用概览

文件名称:	base.apk
文件大小:	10.76MB
应用名称:	冬瓜音乐
软件包名:	com.xifeng.music
主活动:	com.xifeng.music.MainActivity
版本号:	1.0.7
最小SDK:	24
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	56/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	2e1657d5d3fc1d7eca44b7516214ce67
SHA1:	4b1e0d6431717a6782e2bd09f927fe44c637d013
SHA256:	a4c2de503a0c98635b86e4df1ca89bcd71f3f63bcfaa5739d12c2a8378a485e

分析结果严重性分布

高危	中危	信息	安全	关注
0	10	1	1	0

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：3个，其中export的有： 1个
Receiver组件：1个，其中export的有： 1个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

APK已签名

v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=喜凤
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-12 20:09:09+00:00
有效期至: 2124-06-18 20:09:09+00:00
发行人: CN=喜凤
序列号: 0x1
哈希算法: sha256
证书MD5: 8a1b52822281e2147a2176cb1edb777e
证书SHA1: 48c9896e98a9e43a1f9a1cc5b204fc38f3593114
证书SHA256: 62bf55098889a6ffa9b1bf00b7e0436bb620a13ad3c33193e02a1b4df842f4ff
证书SHA512:
50b9d144bd4031ef34f2c7cac1c5b9d0a720f630fdb30faa41dd12b0bec88fba2218c9cd8e9a9af43fe26989655dd6929701e101e79d58e15b11d42b266ef5d3

公钥算法: rsa
密钥长度: 2048
指纹: e1fd2d7fec454767b3f86793559ecfee54774ec944f62b3f99ceebc8f0aa3027
共检测到 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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.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。
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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
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.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.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.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
com.xifeng.music.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.xifeng.music.MainActivity	Schemes: http://, https://, vnd.youtube://, vnd.youtube.launch://, Hosts: youtube.com, m.youtube.com, www.youtube.com, music.youtube.com, youtu.be, Mime Types: text/plain, Path Prefixes: /v/, /embed/, /watch, /channel/, /user/, /c/, /playlist, /,

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: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F0F0003]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Service (com.xifeng.music.playback.MusicService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (androidx.compose.ui.tooling.PreviewActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **6** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
3	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
4	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
5	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
6	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

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/libgushi.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 shell code 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。	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	True info 二进制文件有以下加固函数:['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info 符号被剥离

2	arm64-v8a/libmod_gushi.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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	True info 二进制文件有以下加固函数:['__strncpy_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	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.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_AUDIO

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
nmobi.kuwo.cn	安全	是	**IP地址:** 49.7.249.167 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
wapi.kuwo.cn	安全	是	**IP地址:** 49.7.249.167 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
pipedapi.kavin.rocks	安全	否	**IP地址:** 188.114.96.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333260 **经度:** -87.447083 **查看:** Google 地图
img2.kuwo.cn	安全	是	**IP地址:** 180.105.204.56 **国家:** 中国 **地区:** 中国江苏 **城市:** 徐州 **纬度:** 34.205768 **经度:** 117.284124 **查看:** 高德地图
mobilist.kuwo.cn	安全	是	**IP地址:** 49.7.250.27 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
lx.sycdn.kuwo.cn	安全	是	**IP地址:** 218.93.70.68 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
q1.qlogo.cn	安全	是	**IP地址:** 27.155.118.96 **国家:** 中国 **地区:** 福建 **城市:** 福州市 **纬度:** 26.099774 **经度:** 119.302249 **查看:** 高德地图

api.7a.ink	安全	是	**IP地址:** 81.70.153.134 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
kbangserver.kuwo.cn	安全	是	**IP地址:** 49.7.249.167 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
discord.com	安全	否	**IP地址:** 162.159.136.232 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
ktor.io	安全	否	**IP地址:** 188.114.96.0 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
lrclib.net	安全	否	**IP地址:** 135.181.147.238 **国家:** 芬兰 **地区:** 新地省 **城市:** 赫尔辛基 **纬度:** 60.169521 **经度:** 24.935450 **查看:** Google 地图
static.kuwo.cn	安全	否	No Geolocation information available.
er.sycdn.kuwo.cn	安全	是	**IP地址:** 58.223.176.134 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
www.kuwo.cn	安全	是	**IP地址:** 49.7.250.27 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 17.5.1.21	com/xifeng/innertube/models/U.java
• https://ktor.io/docs/http-client-engines.html	io/ktor/client/d.java
• https://pipedapi.kavin.rocks/streams/	com/xifeng/innertube/c.java
• https://ktor.io/docs/faq.html#no-transformation-found-exception	io/ktor/client/call/c.java
• https://lrclib.net	com/my/kizzy/gateway/f.java
• https://discord.com/login	com/xifeng/music/S.java
• www.manifestations • www.googleorganizationautocompleterequirementsconservative • http://descriptionrelatively • http://www.icon • http://dictionaryperceptionrevolutionfoundationpx;height:successfulsupportersmillenniumhis • www.in • http://s;text-align:centerfont-weight: • http://according • http://style= • http://interested • javascript:constituentwas • http://mathematicsmargin-top:eventually • http://www.language= • http://addeventlistenerresponsible • http://applicationslink • http://ua-compatible • http://familiar • https://www.recent • http://whether • http://staticsuggested • http://imenglish • http://site_name • http://www.hortcut • http://www.style= • http://navigation • http://www.css • https://www.world • http://html4/loose.dtd • http://www-//w3c//dtd • http://xt/css • http://option • http://iparticipation • http://www.wencodeuricomponent • http://interpreted • http://www.c//dtd • http://www.interpretation • http://encoding= • http://www.text-decoration:underline • http://www./div • http://www.years	org/brotli/dec/e.java

• http://wapi.kuwo.cn/api/pc/classify/playlist/gettagplaylist?pn=1&rn=30&id= • https://mobilist.kuwo.cn/list.s?type=songlist&id= • https://www.kuwo.cn/playlist_detail/****** • 4.3.0.8 • http://wapi.kuwo.cn/api/www/bang/bang/musiclist?bangid= • http://er.sycdn.kuwo.cn • https://api.7a.ink/ppmusic/api.php?act=import&url= • https://img2.kuwo.cn/star/albumcover/ • https://wapi.kuwo.cn/api/pc/classify/playlist/gettaglist • http://wapi.kuwo.cn/api/pc/bang/list • https://static.kuwo.cn/kuwomedia/pc/third/img/default.png • https://github.com/z-huang/innertune • https://www.kuwo.cn/openapi/v1/www/search/searchkey?key=&httpsstatus=1 • https://nmobi.kuwo.cn/mobi.s?f=kuwo&q= • https://www.kuwo.cn/api/www/search/searchkey?type=1&httpsstatus=1 • https://www.kuwo.cn/api/www/search/searchkey?key=&httpsstatus=1 • http://kbangserver.kuwo.cn/ksong.s?from=pc&type=bang&id= • https://www.kuwo.cn/api/www/search/searchkey?httpsstatus=1 • https://www.kuwo.cn/search/searchmusicbykeyword?vipver=1&client=kt&ft=music&cluster=0&strategy=2012&encoding=utf8&rformat=json&mobi=1&issubtitle=1&show_copyright_off=1&pn= • https://www.kuwo.cn/ • http://lx.sycdn.kuwo.cn • https://api.7a.ink/ppmusic/donggua.json • http://wapi.kuwo.cn/api/www/playlist/playlistinfo?pid= • https://www.kuwo.cn/api/www/search/hotsearch?type=1&httpsstatus=1 • http://wapi.kuwo.cn/api/pc/classify/playlist/gettagplaylist?pn= • http://api.7a.ink/ppmusic/webs/reward.php • http://wapi.kuwo.cn/api/pc/classify/playlist/getrcmplaylist?pn= • https://q1.qlogo.cn/g?b=qq&nk=727418&s=640 • https://www.kuwo.cn/api/www/search/hotsearch?httpsstatus=1 • http://api.7a.ink/ppmusic/webs/wechat.php • https://www.kuwo.cn/api/www/search/searchmusicbykeyword?ke=	lib/arm64-v8a/libmod_gushi.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Graphics	Google	利用多个 Android 平台版本中的图形工具降低画面延迟。
Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。DataStore 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
Jetpack Compose	Google	Jetpack Compose 是用于构建原生 Android 界面的新工具包。Jetpack Compose 使用更少的代码、强大的工具和直观的 Kotlin API 简化并加快了 Android 上的界面开发。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
this@copy.slice	io/ktor/util/F.java

敏感凭证泄露检测

可能的密钥
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: