



ANDROID 静态分析报告



📱 红叶小说 • v1.1.7

分析日期: 2024-05-23 18:40:44

i应用概览

文件名称:	hybook.apk
文件大小:	11.83MB
应用名称:	红叶小说
软件包名:	com.hongyebook.app
主活动:	io.dcloud.PandoraEntry
版本号:	1.1.7
最小SDK:	19
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	44/100 (中风险)
杀软检测:	8 个杀毒软件报毒
MD5:	b50e90bbb9dad9d35a5626ac30af4a34
SHA1:	19f0b84002dec5762fdeb7cda86ce6212b401f31
SHA256:	f79c5c82deb8ade01fcba84228bdc1844ffb9c0f4026c823cc5c4deb2c0935586

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
4	5	1	2	1

📦四大组件导出状态统计

Activity组件: 9个, 其中export的有: 6个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 2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: OU=com.zhacaibook.reading
签名算法: rsassa_pkcs1v15
有效期自: 2021-09-30 02:25:02+00:00
有效期至: 2046-09-24 02:25:02+00:00
发行人: OU=com.zhacaibook.reading
序列号: 0x6bdf6e5a
哈希算法: sha256
证书MD5: a6c6278552c2841a7e86639043176148
证书SHA1: 389ad2629690b357ef515e53675eea38bef3a8a9
证书SHA256: 6579072a3ed4d608913f9b51f3ec4cc011e71df33c11b11c8c389df00e865dc3
证书SHA512:
d5de779e94ebb89dafeabf1ceeaa8cf6daa08c035480201342047dfc13e528fa86dbeec5aa5f20250bd7b344580656500606bdf2ef0081bb94ff3ea3dcb8413

公钥算法: rsa
密钥长度: 2048
指纹: 6825ace6a837d713a5cdd3e4840209dd98c8aa8a7f0fc01b8557776a5e92ac91
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.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.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.INSTALL_PACKAGES	签名(系统)	请求安装APK	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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.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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要利用到的权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Schemes: qimanwu://

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

Manifest 配置安全分析

高危: 3 | 警告: 1 | 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 4.4-4.4.4, [minSdk=19]	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 (io.dcloud.PandoraEntry) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (io.dcloud.PandoraEntryActivity) 的启动模式不是 standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity (io.dcloud.WebAppActivity) 的启动模式不是 standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

代码安全漏洞检测

高危: 1 | 警告: 3 | 信息: 1 | 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
2	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
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	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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	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	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
---	------------------------------------	----	--	-----------------------------

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)	FORIFY (常用函数加强检查)	SYMBOLS TRIPPED(裁剪符号表)
1	armeabi-v7a/liblame.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。	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。	No info 二进制文件没有设置运行时搜索路径或RPATH	No info 二进制文件没有设置RPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 libc 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	

2	armeabi-v7a/libstatic-webp.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。	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。	No ne info 二进制文件没有设置运行时搜索路径 RPATH	No ne info 二进制文件没有设置 RUNITH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 libc 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/FIutter 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	9/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	8/16	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE

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
----	----	------	------

lame.sf.net	安全	否	IP地址: 104.18.21.237 国家: 美利坚合众国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
ask.dcloud.net.cn	安全	是	IP地址: 58.222.30.203 国家: 中国 地区: 江苏 城市: 台州 纬度: 32.492168 经度: 119.910767 查看: 高德地图

🌐 URL 链接安全分析

URL信息	源码文件
- http://app.cdn.hongyeapp.com/index.php/apiv1/ - https://github.com/indutny/elliptic - https://github.com/indutny/elliptic/issues - https://registry.npmjs.org/elliptic/-/elliptic-6.5.2.tgz - https://github.com/crypto-browserify/crypto-browserify - http://feross.org - https://service.dcloud.net.cn/uniapp/feedback.html	自研引擎
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smart phones, and likely your ATM too.
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。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Weex	Alibaba	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验，来构建 Android、iOS 和 Web 应用。简单来说，在集成了 WeexSDK 之后，你可以使用 JavaScript 语言和前端开发经验来开发移动应用。
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。
---------------	------------------------	------------------------------

 敏感凭证泄露检测

可能的密钥
DCLOUD的 "APPID" : " _UNI_2A301D5"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "com.hongyebook.app _UNI_2A301D5 125066230009 "
DCloud（数字天堂）的=> "DCLOUD_AD_ID" : "1.25066232E11"
DCLOUD的 "AD_ID" : "125066230009"
DCLOUD的 "ApplicationId" : "com.hongyebook.app"
"dcloud_permissions_reauthorization" : "reauthorize"

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患。

© 2025 南明离火 - 移动安全分析平台自动生成