



## ANDROID 静态分析报告



📱 GSLWallet • v1.0.0

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-13 21:15:29

## i应用概览

文件名称:	app.apk
文件大小:	12.54MB
应用名称:	GSLWallet
软件包名:	com.gslwallet
主活动:	io.dcloud.PandoraEntry
版本号:	1.0.0
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
开发框架:	DCloud, Weex
应用程序安全分数:	41/100 (中风险)
杀软检测:	AI评估: 可能有安全隐患
MD5:	620f9b66007682a73d59ba4bd2d16193
SHA1:	36acd146cfb9c4caa69c6e1dd1c9d1e3a3a60c9b
SHA256:	d3098a297392436b412417b2dd0ef752d3780360272a35a358ab996c22c7c73

## 📊 分析结果严重性分布



## 📦 四大组件导出状态统计

Activity组件: 10个, 其中export的有: 0个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 0个
Provider组件: 2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: True  
 v4 签名: False  
 主题: C=CN, ST=, L=, O=Android, OU=Android,  
 CN=%2F3tAlbaJJK9FHFxqDNjnBfVrokFTFAD%2FqOLyYaA7dIRHusWjJVwOjbx6gBPRivxfAKPamLi5r0jtc%2BaVzA5jzw%3D%3D  
 签名算法: rsassa\_pkcs1v15  
 有效期自: 2024-11-12 04:36:10+00:00  
 有效期至: 2124-10-19 04:36:10+00:00  
 发行人: C=CN, ST=, L=, O=Android, OU=Android,  
 CN=%2F3tAlbaJJK9FHFxqDNjnBfVrokFTFAD%2FqOLyYaA7dIRHusWjJVwOjbx6gBPRivxfAKPamLi5r0jtc%2BaVzA5jzw%3D%3D  
 序列号: 0x3b75ab3f  
 哈希算法: sha256  
 证书MD5: 5e94de3408bd75d6857dfa0c7da011d7  
 证书SHA1: 3c22ef495db5ef390a5f41db4178e79498ca1a5f  
 证书SHA256: 4b0e16b900625b54943a86df30f048bab805c06f4af870d9af9125a47c93f8e3  
 证书SHA512:  
 04efd1d5d49265f04186f6a67c6d8c731c14c22edf4cd40d0b07690a56b52354deff6c4df38968e9fe287dd27b5d1dcea77eb537fb8eafa7156d1bcba89c4dc0  
  
 公钥算法: rsa  
 密钥长度: 2048  
 指纹: 7200c5d5123d17c6b8410c9998c5963d7671517839fdd80155a7bab99d1b4936  
 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APP	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.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.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.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.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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在本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，在华硕设备上需要用到的权限。

## 🔒 网络通信安全风险分析

序号	范围	严重程度	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。
2	Activity (io.dcloud.PandoraEntry) 容易受到StrandHogg 2.0的攻击	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。
3	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。
4	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: 0 | 警告: 3 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	<a href="#">应用程序记录日志信息,不得记录敏感信息</a>	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	<a href="#">升级会员: 解锁高级权限</a>
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	<a href="#">升级会员: 解锁高级权限</a>
3	<a href="#">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</a>	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	<a href="#">升级会员: 解锁高级权限</a>
4	<a href="#">MD5是已知存在哈希冲突的弱哈希</a>	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	<a href="#">升级会员: 解锁高级权限</a>

## 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(调用函数加强检查)	SYMBOLS STRIPPED (裁剪符号表)
1	arm64-v8a/liblamemp3.so	<p>True <b>info</b></p> <p>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。</p>	<p>动态共享对象 (DSO) <b>info</b></p> <p>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。</p>	<p>True <b>info</b></p> <p>这个二进制文件在栈上添加了一个栈哨兵，以便它会被溢出返回地址的缓冲区覆盖。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。</p>	<p>Full RELRO <b>info</b></p> <p>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。</p>	<p>No <b>none</b> <b>info</b></p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>No <b>none</b> <b>info</b></p> <p>二进制文件没有设置 RUNPATH</p>	<p>False <b>warning</b></p> <p>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</p>	<p>True <b>info</b></p> <p>符号被剥离</p>

2	arm64-v8a/libstatic-webp.so	<p><b>True info</b></p> <p>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。</p>	<p><b>动态共享对象 (DSO) info</b></p> <p>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。</p>	<p><b>True info</b></p> <p>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</p>	<p><b>Full RELRO info</b></p> <p>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。</p>	<p><b>None info</b></p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>	<p><b>None info</b></p> <p>二进制文件没有设置RUNPATH</p>	<p><b>True info</b></p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memcpy_chk', '_memmove_chk', '_vsprintf_chk']</p>	<p><b>True info</b></p> <p>符号被剥离</p>
---	-----------------------------	--------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------	-------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	--------------------------------------

### 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	<a href="#">升级会员: 解锁高级权限</a>
00063	隐式意图 (查看网页、拨打电话等)	控制	<a href="#">升级会员: 解锁高级权限</a>
00022	从给定的文件绝对路径打开文件	文件	<a href="#">升级会员: 解锁高级权限</a>
00012	读取数据并放入缓冲流	文件	<a href="#">升级会员: 解锁高级权限</a>
00089	连接到 URL 并接收来自服务器的输入流	命令网络	<a href="#">升级会员: 解锁高级权限</a>
00109	连接到 URL 并获取响应代码	网络命令	<a href="#">升级会员: 解锁高级权限</a>
00036	从/res/raw/ 目录获取资源文件	反射	<a href="#">升级会员: 解锁高级权限</a>
00051	通过SetData隐式意图 (查看网页、拨打电话等)	控制	<a href="#">升级会员: 解锁高级权限</a>

### 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.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	10/46	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 android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO

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	<b>IP地址:</b> 104.18.21.237 <b>国家:</b> 美国 <b>地区:</b> 加利福尼亚 <b>城市:</b> 旧金山 <b>纬度:</b> 37.775700 <b>经度:</b> -122.395203 <b>查看:</b> <a href="#">Google 地图</a>

### 🌐 URL 链接安全分析

URL 信息	源码文件
<ul style="list-style-type: none"> <li>https://app.gslwallet.com/?</li> <li>https://service.dcloud.net.cn/uniapp/feedback.html</li> </ul>	自研引擎-A
<ul style="list-style-type: none"> <li>http://lame.sf.net</li> </ul>	lib/arm64-v8a/liblamemp3.so

### 📦 第三方 SDK 组件分析

SDK 名称	开发者	描述信息
MSA SDK	<a href="#">移动安全联盟</a>	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	<a href="#">Facebook</a>	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	<a href="#">Android</a>	在 Android 应用中运行原生代码。

DCloud	<a href="#">数字天堂</a>	libdeflate is a library for fast, whole-buffer DEFLATE-based compression and decompression.
GIFLIB	<a href="#">GIFLIB</a>	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, smartphones, and likely your ATM too.
android-gif-drawable	<a href="#">koral-</a>	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Weex	<a href="#">Alibaba</a>	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	<a href="#">Android</a>	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 或者 file://Uri 以促进安全分享与应用程序关联的文件。

## 🔑 敏感凭证泄露检测

可能的密钥
DCLLOUD的 "AD_ID" : "125758120511"
DCLLOUD的 "APPID" : "_UNI_17237D0"
DCLLOUD的 "CHANNEL" : "common"
DCLLOUD的 "DCLLOUD_STREAMAPP_CHANNEL" : "com.gslwallet _UNI_17237D0_125758120511 common"
DCLLOUD的 "ApplicationId" : "com.gslwallet"
"dcloud_permissions_reauthorization" : "reauthorize"
03686259d5b9d1ac302cd166dd715b7ce

## 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