南明离火
移动应用检测平台

ANDROID 静态分析报告

品质商城 • v1.0

分析日期: 2025-08-28 18:48:13

应用概览

文件名称:	4a26270d9f60e9356a6ba53d141a70a5.apk
文件大小:	1.96MB
应用名称:	品质商城
软件包名:	com.lgehz.tggdo
主活动:	com.tencent.myapplication.MainActivity
版本号:	1.0
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估：安全
MD5:	4a26270d9f60e9356a6ba53d141a70a5
SHA1:	e67a1ef27b5f44253b1a8c7d81525fb284c7539f
SHA256:	556684772385f73c1f987d4487de2e2752ea01cc51f5d64ae34ac36d63d2abae

分析结果严重性分布

高危	中危	信息	安全	关注
2	12	1	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 2个
Service组件：1个，其中export的有： 1个
Receiver组件：1个，其中export的有： 1个
Provider组件：1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: C=US, O=Org_e7bde9, OU=Unit_e7bde9, CN=Random_e7bde9
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-12 08:36:42+00:00
有效期至: 2052-12-28 08:36:42+00:00
发行人: C=US, O=Org_e7bde9, OU=Unit_e7bde9, CN=Random_e7bde9
序列号: 0x1bf28ac0
哈希算法: sha256
证书MD5: ec5a6ea46aa4e0921b0cb0adf8f33d31
证书SHA1: 4339dc5a82e0632e165b0a35a7f515d7b7956b4a
证书SHA256: eb0819bbdf8f7471da70ac741e58b4877040e0d597126d1b464ff8c075a5d985
证书SHA512:
2c754f0c2868d7b25b6235ced572eb9a7899da800e8c533982e0e9d38a3ea220436352a05b170de891a4ba489e0c432f9323b89ae2ca1b4c32473a7fa9c04e24

公钥算法: rsa
密钥长度: 2048
指纹: ee806282b0956fe401f456f75e13cf7572541dbfb618c2a7b9750188b5904fdd
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.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.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
com.lgehz.tggdo.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.tencent.myapplication.MainActivity	Schemes: test://,

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: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
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.tencent.myapplication.service.PayAccessibilityService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	检测到 Service 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。
4	Activity (com.alipay.sdk.app.PayResultActivity) 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	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
6	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: **2** | 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
2	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
3	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
4	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
5	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
6	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
7	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
8	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

9	使用弱加密算法	高危	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

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
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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	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
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00092	发送广播	命令	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	3/46	android.permission.INTERNET 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
mobilegw.dl.alipaydev.com	安全	是	**IP地址:** 110.75.132.25 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
mobilegw.alipaydev.com	安全	是	**IP地址:** 110.75.132.131 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
h5.m.taobao.com	安全	是	**IP地址:** 180.97.251.189 **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

URL 链接安全分析

URL信息	源码文件
• https://mobilegw.alipaydev.com/mgw.htm • https://mobilegw.alipay.com/mgw.htm • https://mobilegw.dl.alipaydev.com/mgw.htm	a0/d.java
• https://mcgw.alipay.com/sdklog.do • https://mobilegw.alipay.com/mgw.htm • https://mobilegw.alipaydev.com/mgw.htm • https://loggw-exsdk.alipay.com/loggw/logupload.do • https://mobilegw.dl.alipaydev.com/mgw.htm	g0/a.java

• 180.76.76.76 • 8.8.8.8 • 114.114.114.114 • 208.67.222.222 • 119.29.29.29 • 1.2.4.8 • 223.5.5.5	v1/B0.java
• https://ds.alipay.com/?from=pc	r1/c.java
• 1.2.4.8	v1/C0404w.java
• http://m.alipay.com/?action=h5quit	M0/AbstractC0318b.java
• https://h5.m.taobao.com/mlapp/olist.html	a0/c.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

敏感凭证泄露检测

可能的密钥
e6b1bdcb890370f2f2419fe06d0fdf7[illegible]0083d52da1ecfe991164[illegible]1b[illegible]f9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c311b4756e1e20877[illegible]89[illegible]4f6[illegible]1bff4bbbc58174d2[illegible]96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843df9434b164e0220baab[illegible]10c8978c3f4c6b7da79d8220a9[illegible]8356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65fdffd2c080281a6ab[illegible]0be587[illegible]e0330eb7ff70871[illegible]e717[illegible]ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7
L3N5cy9jbGFzcy9uZXQvd2xhbjAvYWRkcmVzcw==
Y29tLnRlbmNlbnQuYW5kcm9pZC5xcWRvd25sb2FkZXI=
b6cbad6cbd5ed0d209afc69a[illegible]d3b[illegible]a6[illegible]7efaae9b3c47eabe0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7[illegible]e[illegible]e18f[illegible]5ca98b8ed2eaf86ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649
QrMgt8GGYI6[illegible]62ZY[illegible]hhtxkLzb8egpFn3j5JELI8H6wtACbUnZ5cc3aYTsTRbmkAkRJeYbtx92LPBWm7nBO9UIl7y5i5MQNmUZNf5QENurR5tGyo7yJ2G0MBjW[illegible]AtlA[illegible]cKP0SwOUeUWx5dsBdyhxa7Id1APtybSdDgicBDuNjI0mlZFUzZSS9dmN8lBD0WTVOMz0pRZbR3cysomRXOO1ghqjJdTcyDIxzpNAEszN[illegible]G[illegible]zyU7Hjbmwi6YNK

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隐患。