南明离火
移动应用检测平台

ANDROID 静态分析报告

金投鼎新 v1.0

分析日期: 2025-08-29 16:21:40

应用概览

文件名称:	base_040835.apk
文件大小:	10.72MB
应用名称:	金投鼎新
软件包名:	wild.qz7bk70h.mgl57vn0os
主活动:	wild.qz7bk70h.mgl57vn0os.HomeActivity
版本号:	1.0
最小SDK:	25
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
杀软检测:	AI评估：安全
MD5:	16469287aea64673b6139b68509351cb
SHA1:	cb2b56af4346f46d44c895 1f6edc8826fabbdf1
SHA256:	10e3b36d4a398 71b d73a2ad18739 535f2f3cec0b80fd39272d2e6d

分析结果严重性分布

高危	中危	信息	安全	关注
2	6	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：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：0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=GY, L=Kyiv, O=Travel and Tourism, CN=Travel and Tourism
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-11 05:19:20+00:00
有效期至: 2028-05-07 05:19:20+00:00
发行人: C=GY, L=Kyiv, O=Travel and Tourism, CN=Travel and Tourism
序列号: 0x1989791a046
哈希算法: sha256
证书MD5: a702cf276ed1aeccdcea4cfbaab04b19
证书SHA1: 70c01e67496e0ad22c9772440fc4e8aeffde65aa
证书SHA256: 835d4940aa975cf72d2d36906ca42f56087b1d98ce03475d6e9381e0317c77d2
证书SHA512:
c1a6ad48bff065b070725085dee42995e8b64ef311fa895adc3cd58c7953f8ba7d67a61a4c1f9fb542e687c2a70322a3a97e66c1e03223[illegible]0589fa2c7d17c7ae

公钥算法: rsa
密钥长度: 2048
指纹: db800a4ca815a577d2c85ffcbfc7aae9c79c10c242e0188f18b14c86cdeffca3
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。

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: 3 | 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	Activity (wild.qz7bk70h.mgl57vn0os.MainActivity) 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。

代码安全漏洞检测

高危: **2** | 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	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
2	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
3	应用程序记录日志信息，不应该记录敏感信息	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	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
5	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

6	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。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

应用行为分析

编号	行为	标签	文件
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

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	1/46	android.permission.INTERNET

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。

URL 链接安全分析

URL信息	源码文件
• https://kjur.github.io/jsrsasign/license	自研引擎-A

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

敏感凭证泄露检测

可能的密钥
aHR0cHM6Ly9zbnhqZG0yOGR0eHcuczMtYWNjZWxlcmF0ZS5hbWF6b25hd3MuY29tL3NqeG5kaG4udHh0

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。