南明离火
移动应用检测平台

ANDROID 静态分析报告

MAIDEN • v35.0

分析日期: 2025-03-11 07:11:58

应用概览

文件名称:	74a475c5edd894dc22ce009820ac378c.apk
文件大小:	1.97MB
应用名称:	MAIDEN
软件包名:	com.trade_system.one.maiden
主活动:	com.trade_system.one.maiden.verUpdateActivity
版本号:	35.0
最小SDK:	22
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:	50/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	74a475c5edd894dc22ce009820ac378c
SHA1:	a32c127cc38c869b0e7819c1a736b2b6a2bbd32f
SHA256:	ec81902e77cbc8f5255232d68751ab6bad3eba7929981bd960e9a090475e6ce

分析结果严重性

高危	警告	信息	安全	关注
1	2	1	1	0

四大组件信息

Activity组件：21个，其中export的有：20个
Service组件：1个，其中export的有：1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

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: C=kr, O=KingStock, CN=Chins
签名算法: rsassa_pkcs1v15
有效期自: 2018-03-16 03:55:03+00:00
有效期至: 2043-03-10 03:55:03+00:00
发行人: C=kr, O=KingStock, CN=Chins
序列号: 0x1355a4e8
哈希算法: sha256
证书MD5: af53f1e23aa5b92ab3462895c29bfc96
证书SHA1: d99975778970f74ed782151cd7ce644350822153
证书SHA256: 66c1187f26e220e25183a2d0cbc765c50592f57ff32dd6d4c30cf0e9bc95f4d6
证书SHA512:
b91741a69b3f6e372519b58ee00fa3d27702b19b87f0d2c70c67ed5306405d20eb4385ea60791f389275d69397d61b18cb64a0919f279060b6d717f37731ead4

公钥算法: rsa
密钥长度: 2048
指纹: 717439e7ab69d828ae1b45d3fd1917cdb0bb772568874d952393f807082e8b7a
找到 1 个唯一证书

应用权限

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.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.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.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）

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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分析

高危: 0 | 警告: 22 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

2	Service (com.trade_system.one.maiden.FxService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
3	Activity (com.trade_system.one.maiden.LoginActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (com.trade_system.one.maiden.MainActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (com.trade_system.one.maiden.OrderMgrActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity (com.trade_system.one.maiden.SymbolSearchActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity (com.trade_system.one.maiden.HogaActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity (com.trade_system.one.maiden.DayPLMoneyListActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity (com.trade_system.one.maiden.DepositWithdrawActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Activity (com.trade_system.one.maiden.DepositWithdrawListActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Activity (com.trade_system.one.maiden.OverNightActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity (com.trade_system.one.maiden.SettingsActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
13	Activity (com.trade_system.one.maiden.NoticeListActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Activity (com.trade_system.one.maiden.CustomerChgActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成

15	Activity (com.trade_system.one.maiden.SchOrderListActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Activity (com.trade_system.one.maiden.SignupMemberActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
17	Activity (com.trade_system.one.maiden.SchTradeListActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
18	Activity (com.trade_system.one.maiden.NotiMsgActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
19	Activity (com.trade_system.one.maiden.PossAmountActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
20	Activity (com.trade_system.one.maiden.TermsOfServiceActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
21	Activity (com.trade_system.one.maiden.ChartActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
22	Activity (com.trade_system.one.maiden.SymbolInfoActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

</> 安全漏洞检测

高危: **1** | 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	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	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	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
4	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
5	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	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-2	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息

tvc-invdn-com.investing.com	安全	否	**IP地址:** 104.18.32.151 **国家:** 美国 **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

URL链接分析

URL信息	源码文件
• https://tvc-invdn-com.investing.com/tool/1.12.9/tool-prod-2-ssl.html?carrier=c035992d6b0ce28acd04b3774ddc2101&time=1683522219&domain_id=18&lang_id=18&timezone_id=26&version=1.12.9&locale=ko&timezone=asia/seoul&pair_id=8874&&interval=d&session=24x7&prefix=kr&suffix=_kr&client=0&user=&plotstyle=candles&geoc=kr&styleoverride=	com/trade_system/one/maiden/ChartActivity.java
• 127.0.0.1	com/trade_system/one/maiden/verUpdateActivity.java
• 172.65.197.53	com/trade_system/one/maiden/smclient/SMCLEINTSYS.java
• 1.0.0.2	com/trade_system/one/maiden/util/lib.java

第三方SDK

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。

密钥凭证

可能的密钥
c035992d6b0ce28acd04b3774ddc2101

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。