南明离火
移动应用检测平台

ANDROID 静态分析报告

PuzzleGame • v1.0

分析日期: 2025-04-20 15:24:26

应用概览

文件名称:	Puzzle_Game.apk
文件大小:	6.7MB
应用名称:	PuzzleGame
软件包名:	com.example.puzzlegame
主活动:	com.example.puzzlegame.activity.MainActivity
版本号:	1.0
最小SDK:	28
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	41/100 (中风险)
杀软检测:	AI评估：安全
MD5:	fe796af71f3a9470640073d60cde2950
SHA1:	700731c08a21fa448f88f41e0[illegible]94f37d4e
SHA256:	52556572ef0187124b66f[illegible]b1b0ce52acca60c19d0[illegible]df102142b18afad1a6

分析结果严重性分布

高危	中危	信息	安全	关注
3	[illegible]	0	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有：0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：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: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-09 05:47:38+00:00
有效期至: 2055-03-02 05:47:38+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
证书MD5: 570c94e2f131f4c33b90542a2b29d404
证书SHA1: 58ac0b96267373d459387c4971baccba8c7a4d09
证书SHA256: 084c17af1e1437323c3085deebcc2b017fa5449177e8eee9117f76f8d9a7393a
证书SHA512:
9bf78f5934d7ccedee12724b7c4ac076e666a50233ae6606ed56874dd89dcc1cdcc9f76dcfc55ed1481bd3646e3ea7bcc43afa21e489132226094d84745587f2

公钥算法: rsa
密钥长度: 1024
指纹: 883899a4e8ba1bb1ff7f7f7fb4987952e681fc9982d7e4960749ecf893541b05
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.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。

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: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: **1** | 警告: **1** | 信息: **0** | 通过: **0**

序号	问题	严重程度	描述信息
1	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
2	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。

代码安全漏洞检测

高危: **1** | 警告: **3** | 信息: **0** | 安全: **0** | 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	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
4	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

应用行为分析

编号	行为	标签	文件
00054	从文件安装其他APK	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	1/45	android.permission.WRITE_EXTERNAL_STORAGE

常用: 已知恶意软件经常滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

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。
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。

🔑 敏感凭证泄露检测

可能的密钥
50cc0431350680c30a5ec51952736d0c
d41d8cd98f00b204e9800998ecf8427e

免责声明及风险提示: