



ANDROID 静态分析报告



● 資產相連 · v2.0

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: 2024-10-01 20:15:03

i应用概览

文件名称:	zcxI923rWuZI0wY69JE85vjegb3.apk
文件大小:	1.95MB
应用名称:	資產相連
软件包名:	com.example.app
主活动:	com.example.app.MainActivity
版本号:	2.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	64/100 (低风险)
杀软检测:	AI评估: 安全
MD5:	52fed636926ec80a9a88c2a207b5748a
SHA1:	6dbf363e95ab7a3cfc7aaec103692ad262c693ee
SHA256:	b8b006cf167745430366691fd66c8cbbbd75cf17d146d7b05809238d60323f7d0

分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
0	4	2	1	0

四大组件信息

Activity组件: 1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: 0个, 其中export的有: 0个

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: C=TG@apksigner, ST=TG@apksigner, L=TG@apksigner, O=eu1727784038490, OU=mn1727784038490, CN=sigs
 签名算法: rsassa_pkcs1v15
 有效期自: 2024-10-01 12:00:38+00:00
 有效期至: 2074-09-19 12:00:38+00:00
 发行人: C=TG@apksigner, ST=TG@apksigner, L=TG@apksigner, O=eu1727784038490, OU=mn1727784038490, CN=sigs
 序列号: 0x10f94f02
 哈希算法: sha1
 证书MD5: 593cc12e365b5b331b688f62c56d8b94
 证书SHA1: a3aa72684ba082ff63b0a6be982402da6a6e682d
 证书SHA256: 257f3e596b5cf577cd62e03648699e8b984e5bd4d5d970e182041c37f6fff039
 证书SHA512:
 e1aba0ca66e232bdb2388d6dfb7de64672fb7318a072236ed629a7d9d1e4b25241cf92a4659b5cc2f61d97104572bfbac2e6936949c03d77bb8a6c66d01ccc3e

公钥算法: rsa
 密钥长度: 1024
 指纹: 4e44f8baf2a418752f28aa74136deeba1e959be359e9bdc78c4c195c077c4b09
 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.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.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.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_CLIPBOARD_IN_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.example.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名

MANIFEST分析

高危: 0 | 警告: 2 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息

1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	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。

</> 安全漏洞检测

高危: 0 | 警告: 2 | 信息: 2 | 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: MST G-STORAGE-3	升级会员: 解锁高级权限
2	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板, 因为其他应用程序可以访问它	信息	OWASP MASVS: MST G-STORAGE-10	升级会员: 解锁高级权限
3	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: MST G-STORAGE-2	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-349: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MST C-PLATFORM-7	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.CAMERA
其它常用权限	3/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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
www.yhjj.cc	安全	否	IP地址: 154.194.64.167 国家: 美利坚合众国 地区: - 城市: - 纬度: 40.712791 经度: -74.006065 查看: Google 地图

🌐 URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://www.yhjj.cc/ 	com/example/app/MainActivity.java
<ul style="list-style-type: none"> https://www.yhjj.cc/ 	自研引擎-S

☰ 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。

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