南明离火
移动应用检测平台

ANDROID 静态分析报告

PIP Photo Editor - v1.0

分析日期: 2024-05-23 06:12:03

应用概览

文件名称:	991c7d6143d3fa4aeb41e7f2038ae7bcc4fb67881d0a2a66ac5fbbc30c7b85a2.apk
文件大小:	17.39MB
应用名称:	PIP Photo Editor
软件包名:	com.pip.photo.editor.camera.pipimage.maker
主活动:	com.pip.photo.editor.camera.pipimage.maker.Splash
版本号:	1.0
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	61/100 (低风险)
杀软检测:	3 个杀毒软件报毒
MD5:	854b5efcec840651e6a5abcde6791573
SHA1:	6ffd984b98a7300932c4b1308e97b0fe493611bdd
SHA256:	991c7d6143d3fa4aeb41e7f2038ae7bcc4fb67881d0a2a66ac5fbbc30c7b85a2

分析结果严重性分布

高危	中危	信息	安全	关注
0	5	1	1	0

四大组件导出状态统计

Activity组件：13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

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True

v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-12 13:20:19+00:00
有效期至: 2051-10-12 13:20:19+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x8e3581a9ccf121018a4c7284c65f8a36dc76e46b
哈希算法: sha256
证书MD5: 464eff02f0989d3f61c57d57d706382b
证书SHA1: cb3e714c8552ac0a0831851679ae61276c32dc29
证书SHA256: 54b8b4015e301f37148281b09a49fe78419e22e5fced1ed6289992bdc585ff9a
证书SHA512:
02a1f732be9dc13a67754b6e09bd94123859b5eaf8fb104019ac1d66cabd24f067690cf8adb3eaa59240fd0ee14ca5437db71e9f231f8487d6efc2a813fc980

公钥算法: rsa
密钥长度: 4096
指纹: 48cd58dbc3f01b75ad1114893923d440ef13ba389b09238ab4ef8aa2b97d48f8
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。
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.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: **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: **1** | 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: **0** | 警告: **4** | 信息: **1** | 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: MSTG-STORAGE-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
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
5	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

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.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE 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。

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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

免责声明及风险提示: