南明离火
移动应用检测平台

ANDROID 静态分析报告

视频嵌入 • v1.0.0

分析日期: 2024-05-30 22:54:21

应用概览

文件名称:	视频嵌入_1.0.0.apk
文件大小:	24.11MB
应用名称:	视频嵌入
软件包名:	com.example.fsjx.shipin.shipinchuli
主活动:	com.example.fsjx.shipin.shipinchuli.MainActivity
版本号:	1.0.0
最小SDK:	21
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	46/100 (中风险)
杀软检测:	AI评估：安全
MD5:	5c3cb5fb860b5f4a5adc637e125f34ca
SHA1:	dea5016ad2a4d6e02872e52dc240ef[illegible]ad59232
SHA256:	b67ce3f38be37bd4e395d6812[illegible]c485ec0bf39ecb30b63[illegible]7996dc7d9c299d4

分析结果严重性分布

高危	中危	信息	安全	关注
2	5	4	1	1

四大组件导出状态统计

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

应用签名证书信息

二进制文件已签名
v1 签名: True

本报告由南明离火移动安全分析平台生成

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: 2023-08-31 13:20:27+00:00
有效期至: 2053-08-23 13:20:27+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha1
证书MD5: 59d3928c97822b7c041a51bbde528bce
证书SHA1: e23ee49cbff6e9ef53e576b87b4c0d3e843f1760
证书SHA256: 2e3163aacbf8d842dcc5ef6798822730d3a741f5aaad50ea77893ec4d0eec602
证书SHA512:
fc3f928763448b0f3fba50f4e86dbccce32ee34eddce4e783ef6d18d211031273afcfb37ede9a6554cf91652caea53aa712bc[illegible]ef1ef6b8fbc13f771f9127

公钥算法: rsa
密钥长度: 2048
指纹: d40f2171fcce73af9193560a1c91c9452d4502b077bfc47617c25ad02cc409ba
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.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.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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
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。

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	应用程序已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: **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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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: **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	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
4	应用程序使用带PKCS5/PKCS7填充的加密模式CBC，此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

5	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libapp.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的shellcode不可执行		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Not Applicable info RELRO检查不适用于Flutter/Dart二进制文件	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False info 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	严重	权限
恶意软件常用权限	1/30	android.permission.READ_PHONE_STATE

其它常用权限	6/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.ACCESS_NETWORK_STATE

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
default.url	安全	否	No Geolocation information available.
dashif.org	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
aomedia.org	安全	否	**IP地址:** 185.199.109.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	a2/a.java
• https://default.url/	k1/n0.java
• data:cs:audioPurposecs:2007 • http://dashif.org/guidelines/thumbnail_tile • http://dashif.org/thumbnail_tile • http://dashif.org/guidelines/trickmode • http://dashif.org/guidelines/last-segment-number • file:dvb-dash:	m2/d.java

• https://aomedia.org/emsg/id3 • data:cs:audiopurposecs:2007 • http://dashif.org/guidelines/thumbnail_tile • https://default.url • http://dashif.org/thumbnail_tile • http://dashif.org/guidelines/last-segment-number • http://dashif.org/guidelines/trickmode • https://developer.apple.com/streaming/emsg-id3 • file:dvb-dash:	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。

敏感凭证泄露检测

可能的密钥
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
e2719d58-a985-b3c9-781a-b030af78d30e
9a04f079-9840-4286-ab92-e65be0885f95
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

免责声明及风险提示: