南明离火
移动应用检测平台

ANDROID 静态分析报告

JVID • v1.0.1

分析日期: 2024-06-24 21:28:25

应用概览

文件名称:	VVKK3328.apk
文件大小:	28.74MB
应用名称:	JVID
软件包名:	com.avasdasdaa.flutter_sf57
主活动:	com.avasdasdaa.flutter_sf57.MainActivity
版本号:	1.0.1
最小SDK:	21
目标SDK:	34
加固信息:	Flutter/Dart 加固
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	a6fd254f7670e760fb2328905409c28b
SHA1:	fc529857074db29e8f8cf7cceb173c43d5dc156f
SHA256:	0f4a3a33ede27637487593d1659711d4327ac95cf8617f5a22e759ad68b620

分析结果严重性分布

高危	中危	信息	安全	关注
1	32	11	2	0

四大组件导出状态统计

Activity组件：4个，其中export的有：16个
Service组件：5个，其中export的有：1个
Receiver组件：9个，其中export的有：8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: True
v2 签名: True

v3 签名: False
v4 签名: False
主题: CN=33, OU=22, O=11, L=233, ST=23, C=2323
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-01 03:57:32+00:00
有效期至: 2049-05-26 03:57:32+00:00
发行人: CN=33, OU=22, O=11, L=233, ST=23, C=2323
序列号: 0x1
哈希算法: sha256
证书MD5: 868e7837ed251c2c8fe4270e1ea6f805
证书SHA1: bf95e7bf2c30fd01bd083d1001c28395917e6af1
证书SHA256: 42890b72cdd5ee993510334369dfa0d80fb07f0f268d1145a1317b3116fb7731
证书SHA512:
5f0781610ff7a1a37199c82624a23a77f62e8d5addf3ff92119979f5ffb9fad364b9b2b0c784e1a824b17a482c34c1a3dabe597219bd4b059d3677e6a85ade60

公钥算法: rsa
密钥长度: 2048
指纹: b43e94eff5a952d4a8849d08eee6272b1745ef2c7872ca335814ffc6261e9337
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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.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_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_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.ADD_VOICEMAIL	危险	将语音邮件添加到系统	允许应用程序将语音邮件添加到系统中。
android.permission.USE_SIP	危险	收听/发出网络电话	允许应用程序使用SIP服务拨打接听互联网通话。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录

android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.ACCESS_MEDIA_LOCATION	危险	获取照片的地址信息	更换头像，聊天图片等图片的地址信息被读取。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.startForegrou...，用于podcast播放（推送悬浮播放，锁屏播放）
com.avasdasdaa.flutter_sf57.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: **26** | 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 9.0-5.0.2, [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。

3	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityDzdp) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
4	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityDy) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
5	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityIns) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
6	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityQq) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
7	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityFacebook) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
8	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityZh) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
9	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityQqmail) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
10	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityXhs) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
11	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityWx) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
12	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityWb) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
13	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityTuite) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
14	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityTb) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。

本报告由南明离火移动安全分析平台生成

15	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityMm) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
16	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityKs) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
17	Activity-Alias (com.avasdasdaa.flutter_sf57.NewActivityJsq) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
18	Activity-Alias (com.avasdasdaa.flutter_sf57.DefaultAlias) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity-Alias是显式导出的。
19	Service (com.google.android.gms.metadata.ModuleDependencies) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
20	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
21	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
22	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
23	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
24	Broadcast Receiver (androidx.work.impl.background.systemalarm.RescheduleReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。

25	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
26	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
27	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **1** | 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
3	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
4	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

5	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
6	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
7	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
8	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	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	匹配	权限
恶意软件常用权限	9/30	android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.CALL_PHONE android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	8/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
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

docs.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
dashif.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
default.url	安全	否	No Geolocation information available.
journeyapps.com	安全	否	**IP地址:** 13.225.131.42 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/baseflow/flutter-permission-handler/issues	l1/t.java
• https://default.url	o3/n0.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	e4/a.java
• http://dashif.org/guidelines/last-segment-number • file:dvb-dash: • data:cs:audiopurposecs:2007 • http://dashif.org/guidelines/thumbnail_tile • http://dashif.org/guidelines/trickmode • http://dashif.org/thumbnail_tile	q4/d.java
• https://default.url • http://dashif.org/thumbnail_tile • file:dvb-dash: • https://aomedia.org/emsg/id3 • data:cs:audiopurposecs:2007 • https://github.com/journeyapps/zxing-android-embedded • http://dashif.org/guidelines/trickmode • https://journeyapps.com/ • http://dashif.org/guidelines/thumbnail_tile • https://github.com/baseflow/flutter-permission-handler/issues • https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures • https://developer.apple.com/streaming/emsg-id3 • http://dashif.org/guidelines/last-segment-number	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。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
Jetpack Camera2	Google	Camera2 is the latest low-level Android camera package and replaces the deprecated Camera class. Camera2 provides in-depth controls for complex use cases, but requires you to manage device-specific configurations.
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

敏感凭证泄露检测

可能的密钥
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"library_zxingandroidembedded_author" : "JourneyApps"
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
e2719d58-a985-b3c9-781a-b030af78d30e
9a04f079-9840-4286-ab92-e65be0885f95
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

免责声明及风险提示: