南明离火
移动应用检测平台

ANDROID 静态分析报告

FLAI • v1.0.14

分析日期: 2024-05-31 15:32:27

应用概览

文件名称:	flai_official_1.0.14_34.apk
文件大小:	38.91MB
应用名称:	FLAI
软件包名:	com.flai.flai
主活动:	com.flai.flai.MainActivity
版本号:	1.0.14
最小SDK:	19
目标SDK:	33
加固信息:	360加固 加固
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	32d2f29977da3b0f1f58da91b0e1af77
SHA1:	b85f96937b905c43ae5b5699228[illegible]4d4ad29f48eb
SHA256:	b04490014a0f9ca5cd8f1b5[illegible]1e7613d032d1a[illegible]f65876e2993eee6c6

分析结果严重性分布

高危	中危	信息	安全	关注
1	9	1	1	3

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：4个，其中export的有：0个
Receiver组件：2个，其中export的有：0个
Provider组件：2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: CN=flai, OU=flai, O=flai, L=taipei, ST=taiwan
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-05 04:34:47+00:00
有效期至: 2048-11-28 04:34:47+00:00
发行人: CN=flai, OU=flai, O=flai, L=taipei, ST=taiwan
序列号: 0x1
哈希算法: sha256
证书MD5: 74ecb2f075fd63c2da6493ef3cd13693
证书SHA1: 209c25ac56eb9bdf2054119972bb59c7dff60c73
证书SHA256: ecb0084ee691d4665c7546ed3f11cc3056663bccf7ccc0b2cf1128c2979785dc
证书SHA512:
de9bc7f2bcb9238e0820a737bb7ddd1be5275f4b65eae892db1ed532826838022ff42a9274cb1b6d446fb0129e5cfb41aa5902c0a44c2b9bb3b25ab69140e330

公钥算法: rsa
密钥长度: 2048
指纹: cc1b80008ef6645de0d7441ad1e0268bfc072e984f9038d6ced32351463a549c
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.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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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_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。
com.flai.flai.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: **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 4.4-4.4.4, [minSdk=19]	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: **6** | 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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
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

6	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
7	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
8	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
9	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

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
2	arm64-v8a/librive_text.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	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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	True info 二进制文件有以下加固函数: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strncpy_chk', '__memmove_chk']	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	1/30	android.permission.READ_PHONE_STATE
其它常用权限	6/46	android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE

常用: 已知恶意软件广泛滥用的权限。

本报告由南明离火移动安全分析平台生成

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
api.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	是	**IP地址:** 180.163.150.34 **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	是	**IP地址:** 180.163.150.34 **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
default.url	安全	否	No Geolocation information available.
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://default.url	w2/n0.java
• http://dashif.org/thumbnail_tile • http://dashif.org/guidelines/trickmode • file:dvb-dash: • http://dashif.org/guidelines/thumbnail_tile • data:cs:audiopurposecs:2007 • http://dashif.org/guidelines/last-segment-number	y3/d.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	m3/a.java
• https://github.com/flutter/packages/blob/main/packages/in_app_purchase/in_app_purchase/readme.md#loading-products-for-sale	n8/i.java

• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	i6/f.java
• https://%s/%s/%s	w6/c.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	b6/t.java
• https://github.com/baseflow/flutter-permission-handler/issues	b0/u.java
• https://play.google.com/store/apps/details?id=	o7/d.java
• https://plus.google.com/	x4/j1.java
• https://api.flutter.dev/flutter/material/scaffold/of.html	lib/arm64-v8a/libapp.so

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。
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包、内存抓取等威胁。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

敏感凭证泄露检测

可能的密钥
"google_crash_reporting_api_key" : "AIzaSyDxrIATpwHsDwMBHGqy8enFPDmntkSUqck"
"google_api_key" : "AIzaSyDxrIATpwHsDwMBHGqy8enFPDmntkSUqck"
470fa2b4ae81cd56ecbcda5735803434cec591fa
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

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，深入扫描软件中中潜在的漏洞和安全隐隐患。