南明离火
移动应用检测平台

ANDROID 静态分析报告

暗网禁地 • v3.0.7

分析日期: 2024-06-24 19:15:27

应用概览

文件名称:	app-aw-0619-v307.apk
文件大小:	17.12MB
应用名称:	暗网禁地
软件包名:	com.anwang_jinqu.app
主活动:	com.anwang_jinqu.app.MainActivity
版本号:	3.0.7
最小SDK:	19
目标SDK:	33
加固信息:	Flutter/Dart 加固
应用程序安全分数:	40/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	03508f25d54aca33b1db246a70341ee4
SHA1:	fd309ccf15688787779172cd597[illegible]adbb6
SHA256:	75159d0758f768a551bff97782[illegible]edd19cbcb8619ab480[illegible]da187be1fcbdba

分析结果严重性分布

高危	中危	信息	安全	关注
4	8	1	1	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 0个
Service组件：0个，其中export的有： 0个
Receiver组件：2个，其中export的有： 1个
Provider组件：3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: C=14000, ST=Phnom Penh, L=Phnom Penh, O=M53, OU=M53, CN=Mr Right
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-26 06:19:47+00:00
有效期至: 2051-06-13 06:19:47+00:00
发行人: C=14000, ST=Phnom Penh, L=Phnom Penh, O=M53, OU=M53, CN=Mr Right
序列号: 0x382f5067
哈希算法: sha256
证书MD5: e2d568ebf9f46fa8738ffef3ef928d8b
证书SHA1: d32888414c09bedaae1a9a2d13f2f5208e65afbd
证书SHA256: 328b79f562eb776ab2c8aa69d2d639f2b757d20fc24fc1e68b74091463b3358f
证书SHA512:
f37dd0fb856005f950ccb2d511826c89a343f9b556db8c6b174eb4fe6f30bc9e72e9ff00d3df376b89916053fedff6fde75d4c0fd2ea10f8f422f53f1ecc1f3d

公钥算法: rsa
密钥长度: 2048
指纹: a6b0d3d1342b63fd4dc90a946b6114224b5462ff18df4de46d72b9733924dfe8
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.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.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.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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.anwang.jinqu.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.anwang.jinqu.app.MainActivity	Schemes: ttk9yx://,

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: **2** | 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 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。
3	Activity (com.pichillilorenzo.flutter_inappwebview_android.chrome_custom_tabs.ChromeCustomTabsActivitySingleInstance) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity (com.pichillilorenzo.flutter_inappwebview_android.chrome_custom_tabs.TrustedWebActivitySingleInstance) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	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: **2** | 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

本报告由南明离火移动安全分析平台生成

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	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
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	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	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
7	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

8	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES

其它常用权限	4/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET 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
dashif.org	安全	否	**IP地址:** 185.199.110.153 **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
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
default.url	安全	否	No Geolocation information available.
aomedia.org	安全	否	**IP地址:** 185.199.111.153 **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
• 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	e2/d.java
• https://aomedia.org/emsg/id3 • https://developer.apple.com/streaming/emsg-id3	s1/a.java
• https://default.url	c1/n0.java

• https://default.url • http://dashif.org/guidelines/last-segment-number • file:dvb-dash: • data:cs:audiopurposecs:2007 • https://aomedia.org/emsg/id3 • http://dashif.org/guidelines/thumbnail_tile • http://dashif.org/guidelines/trickmode • https://developer.apple.com/streaming/emsg-id3 • http://dashif.org/thumbnail_tile	自研引擎-S
• 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。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、Danmaku-FlameMaster 架构清晰、简单易用等优势。
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 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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

敏感凭证泄露检测

可能的密钥
openinstall统计的=> "com.openinstall.APP_KEY" : "ttk9yx"
L3N5c3RlbS9ldGMvZhjbHVkZWQtaW5wdXQtZGV2aWNlcy54bWw=
9a04f079-984[illegible]-e65be0885f95
L3N5c3RlbS9saWIvbGliY2xjb3JlX3g4NF5vw==
YW5kcm9pZC5oYXJkd2FyZSUbHVldG9vdGg=
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
L3N5c3RlbS9iaW4vZHVaWQ0eC1wcm9w
L3N5c3RlbS9mcmFtZXdvcmsveDg2XzY0
L3N5c3RlbS9iaW4vZ2VueW1vdGlvbi12Ym94LXNm

e2719d58-a985-b3c9-781a-b030af78d30e
L3N5cy9jbGFzcy9uZXQvd2xhbjAvYWRkcmVzcw==
L3N5c3RlbS9saWI2NC9saWJjbGNvcmVfeDg2LmJj
L3N5c3RlbS9iaW4vbmVtdVZNLXByb3A=
VGhpcyBpcyB0aGUgcHJlZmI4IGZvciBCaWdJbnRlZ2Vy
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
Y29tLnRlbmNlbnQuYW5kcm9pZC5xcWRvd25sb2FkZXI=
YW5kcm9pZC5oYXJkd2FyZS5jYW1lcmEuZmxhc2g=
L3N5c3RlbS9iaW4vbWljcm92aXJ0LXByb3A=

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。