



ANDROID 静态分析报告



91淫母 · v1.0.0

本报告由南明离火移动安全分析平台生成

本报告由南明离火移动安全分析平台生成

分析日期: 2025-06-20 20:59:21

i应用概览

文件名称:	91yinmugf.apk
文件大小:	17.34MB
应用名称:	91淫母
软件包名:	f0f1d.f8dc7979.fe23db
主活动:	com.app_main.app.MainActivity
版本号:	1.0.0
最小SDK:	19
目标SDK:	33
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	40/100 (中风险)
杀软检测:	AI评估: 安全
MD5:	f4a4cef8fad3e6459191584507c51e12
SHA1:	63232f159910478541c7b16057c57da49f3fc97c
SHA256:	f98f2877f315179df2351e118e13ec4811af9772b2770cf3b7707c4928f6ac47

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 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: 6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: True

v4 签名: None

主题: C=FM, ST=doYong, L=wooBo, O=Aon, OU=Aon, CN=Aon

签名算法: rsassa_pkcs1v15

有效期自: 2024-06-24 08:08:31+00:00

有效期至: 2124-05-31 08:08:31+00:00

发行人: C=FM, ST=doYong, L=wooBo, O=Aon, OU=Aon, CN=Aon

序列号: 0x1cb4e771

哈希算法: sha512

证书MD5: 52135acf35454db41874e484ce42a957

证书SHA1: c4689f95bd6f3029321906d4ba1a35fea4ffef7e

证书SHA256: f5fc2320c229b8325e22818adfff504c3399d1915384b5fb6eb9ed1d8ba84833

证书SHA512:

8ff317a73814e2507eddf8a12d7ade561292bb9bfc781a97cdd0d7851f3f5cdc0c20d86b3b9535c4526e904acf43f419bd4491153d06670b08110b34437a53c

公钥算法: rsa

密钥长度: 2048

指纹: 29aa1b44544a835a2e3694b63776ff6d41082ecd38327ae0cfc0cbaf50d47bb9

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。
f0f1d.f8dc7979.fe23db.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.app_main.app.MainActivity	Schemes: ivuxa2://,

🔒 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。
2	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。
3	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。
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 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: 5 | 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: MST G-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: MST G-STORAGE-2	升级会员: 解锁高级权限
3	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: MST G-CRYPTO-6	升级会员: 解锁高级权限
4	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: MST G-PLATFORM-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: MST G-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: MST G-CRYPTO-3	升级会员: 解锁高级权限
7	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

8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-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 TRIPPED(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。	动态共享对象(DSO) info 共享库是使用fPIC标志构建的，该标志启用与地址无关的编程(ROP)攻击更难可靠地执行。	True info 这个二进制文件在二进制文件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libc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	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入JSON对象	文件	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00028	从 assets 目录中读取文件	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限

00108	从给定的 URL 读取输入流	网络命令	升级会员: 解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络命令	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	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.
aomedia.org	安全	否	IP地址: 185.199.108.153 国家: 美国 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

URL 链接安全分析

L3N5c3RlB59saWlVbGliY2xjb3JlX3g4Ni5iYw==
Y29tLnRlbnNlbnQuYW5kcm9pZC5xcWRvd25sb2FkZXI=
L3N5c3RlB59iaW4vbWljcm92aXJ0LXByb3A=
YW5kcm9pZC5oYXJkd2FyZS5jYW1lcmEuZmxhc2g=
L3N5c3RlB59iaW4vZHJvaWQ0eC1wcm9w
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
L3N5c3RlB59iaW4vZ2VueW1vdGlvbi12Ym94LXNm
L3N5cy9jbGFzcy9uZXQvd2xhbjAvYWRkcmVzcw==

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成