



ANDROID 静态分析报告



闪隐空间 • v1.0

分析日期: 2025-04-16 08:04:15

i应用概览

文件名称:	闪隐空间 v1.0.apk
文件大小:	9.0MB
应用名称:	闪隐空间
软件包名:	fdacfaeo.facbccbp.jifgcefq
主活动:	fdacfaeo.facbccbp.jifgcefq.ui.login.LoginActivity
版本号:	1.0
最小SDK:	24
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	1/432
杀软检测:	16 个杀毒软件报毒
MD5:	d0f9ada383f4080e250c90d69caef980
SHA1:	81ffe6b7c3ece07f5b297bd88ffb39b3c76b646d
SHA256:	07e7e0766615b852d39d5c16b83657928610608f0300a08d932fed49166261cf

分析结果严重性分布

🔴 高危	🟡 中危	📘 信息	🟢 安全	🔍 关注
1	8	1	1	0

四大组件导出状态统计

Activity组件: 3个, 其中export的有: 2个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 1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: False
 v2 签名: True
 v3 签名: True
 v4 签名: False
 主题: C=cn, ST=cihbfbad, L=hidhfbac, O=ahbdiafb, OU=hfedfida, CN=bcbgaagt
 签名算法: rsassa_pkcs1v15
 有效期自: 2024-03-07 05:11:50+00:00
 有效期至: 2124-02-12 05:11:50+00:00
 发行人: C=cn, ST=cihbfbad, L=hidhfbac, O=ahbdiafb, OU=hfedfida, CN=bcbgaagt
 序列号: 0x516dc18f
 哈希算法: sha256
 证书MD5: 1ac5a0e591b2f95b90aea5c122f5ad02
 证书SHA1: 528a26313fd4baaa2b8a321cbf79afade98cf138
 证书SHA256: 0e65c0d1cdda0b2b4e4bdf7fa00bde8e686f73382aa38c2e4b787dbb575b5972
 证书SHA512:
 a0010af311c4c9cf23720bd42eb11590d6e4a970f5234c12f64e518a90f7ff066bec1e9679b9ba53ec76d636bba5bbcb3a1c8b60c41b915648ef815b548186589

 公钥算法: rsa
 密钥长度: 1024
 指纹: 69d7fda25062dd36c2b64bf2e305fb879a505cda8508dfef436e55536982b76a
 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.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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.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.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_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
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.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS_COARSE_LOCATION或ACCESS_FINE_LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令。恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ_PHONE_STATE授予的功能的一个子集，但对即时应用程序公开。
fdacfaeo.facbccbp.jifgcefq.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

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

📜 证书安全合规分析

高危: 0 | 警告: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

🔍 Manifest 配置安全分析

高危: 0 | 警告: 4 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序启用明文网络流量 [android:usesCleartextTraffic="true"]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。

2	应用程序具有网络安全配置 [android:networkSecurityCo nfig=@xml/network_securit y_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	Activity (fdacfaeo.facbccbp.j ifgcefq.ui.splash.SplashActiv ity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (fdacfaeo.facbccbp.j ifgcefq.MainActivity) 未被保 护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Broadcast Receiver (androi dx.profileinstaller.ProfileIns tallReceiver) 受权限保护，但 是应该检查权限的保护级别。 Permission: android.permis sion.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。它受到一个被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，并与其组件交互。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: 0 | 警告: 3 | 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-132: 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	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
4	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
5	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
00067	查询IMSI号码	信息收集	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
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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	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	8/30	android.permission.CAMERA android.permission.WRITE_CONTACTS android.permission.READ_SMS android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.READ_MEDIA_IMAGES

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
hxlm001.icu	安全	否	No Geolocation information available.
www.yiyaoit.top	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
http://www.yiyaoit.top/curtaincalculator/file	fdacfaeo/facbccbp/jifgcefq/net/Apiconfig.java
http://hxlm001.icu/api/uploads/	fdacfaeo/facbccbp/jifgcefq/net/NetConstant.java
http://43.132.236.238/api/uploads/	fdacfaeo/facbccbp/jifgcefq/net/RetrofitHelper.java
http://154.12.31.98/api/uploads/	fdacfaeo/facbccbp/jifgcefq/net/HttpManager.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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，高效的方法在应用程序启动时初始化组件。库开发人员 and 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。
AndroidAutoSize	JesseYanCoding	今日头条屏幕适配方案终极版，一个极低成本 Android 屏幕适配方案。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

敏感凭证泄露检测

可能的密钥
高德地图的=> "com.amap.api.v2.apikey" : "c14406e874f2395cabf68312e06f2fc6"

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

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