南明离火
移动应用检测平台

ANDROID 静态分析报告

ЦБРФ • v2.4.29

分析日期: 2025-08-01 13:44:46

应用概览

文件名称:	base.apk
文件大小:	3.94MB
应用名称:	ЦБРФ
软件包名:	de.nfc_problems.top.once
主活动:	de.tu_darmstadt.seemoo.nfcgate.gui.MainActivity
版本号:	2.4.29
最小SDK:	21
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	67/100 (低风险)
杀软检测:	29 个杀毒软件报毒
MD5:	b8f570c49dac7ec0efbfe76239a08ffd
SHA1:	0f5edcbd4e3340ed2b18705d7ec37a27ec2444a8
SHA256:	c4eeb03ecfb10d93b4635741bdd999910c3f87f99b004d3943c0398c77dc8324

分析结果严重性分布

高危	中危	信息	安全	关注
0	6	1	2	0

四大组件导出状态统计

Activity组件：1个，其中export的有： 0个
Service组件：2个，其中export的有： 1个
Receiver组件：1个，其中export的有： 1个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=DE, ST=Berlin, L=Berlin, O=Unity, OU=Sparrow, CN=Jack
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-12 14:24:17+00:00
有效期至: 2052-07-28 14:24:17+00:00
发行人: C=DE, ST=Berlin, L=Berlin, O=Unity, OU=Sparrow, CN=Jack
序列号: 0x7e1df60098e618ba
哈希算法: sha256
证书MD5: a992db58466ab242603fdeafe5dfad06
证书SHA1: e00afef281f475c43d3fa5783847892983cd6de9
证书SHA256: e5fbe4bae930b0d211183b6e1ba9673f0388b20391c57841ed39481a55151481
证书SHA512:
16a9f6feabbea25b1795266d032ea7f105f3d80dd2fe6ba757c861a6fd2e9f33fd0c3ea1fd1b96f48d749639a8969 7d0057a43199f0b5b0 a950b4bc1202b2ed

公钥算法: rsa
密钥长度: 2048
指纹: 502574c37daa5cb5b624310bd323aa761aeb7e11a104cadb09572f169bfec8cc
共检测到 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.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
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.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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
de.tu_darmstadt.seemoo.nfcgate.top_up.1DYNAMIC_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: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用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: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Service (de.tu_darmstadt.seemoo.nfcgate.nfc.hce.ApduService) 受权限保护，但应检查权限保护级别。Permission: android.permission.BIND_NFC_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
2	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

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-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
3	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
4	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
5	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

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
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
00163	创建新的 Socket 并连接到它	socket	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	0/30	
其它常用权限	4/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET

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。

URL 链接安全分析

URL信息	源码文件
• 10.0.7.106	de/tu_darmstadt/seemoo/nfcgate/BuildConfig.java
• 10.0.7.106	de/tu_darmstadt/seemoo/nfcgate/util/Globals.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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
59ebfcb9a4cb945ecc5cf04b9a6cce1a
2858dd39e73c190fcae137a225c423b6

免责声明及风险提示: