南明离火
移动应用检测平台

ANDROID 静态分析报告

NekoBox : v1.3.8

分析日期: 2025-07-05 23:42:54

应用概览

文件名称:	NekoBox-1.3.8-arm64-v8a.apk
文件大小:	14.37MB
应用名称:	NekoBox
软件包名:	moe.nb4a
主活动:	io.nekohasekai.sagernet.ui.MainActivity
版本号:	1.3.8
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:	51/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	9b589a81eb79422b2850abd6a59db4d9
SHA1:	b22f7a7952347591d3d7c4a463d4ec0ea5a78e17
SHA256:	e3468d2c9c5ee0c8a63817f82f7e9530c184f73b20340b65328e5f33cb5c25ac0

分析结果严重性分布

高危	中危	信息	安全	关注
1	14	2	1	1

四大组件导出状态统计

Activity组件：32个，其中export的有： 1个
Service组件：8个，其中export的有： 2个
Receiver组件：10个，其中export的有： 3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: False
v4 签名: False
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2021-11-27 15:39:36+00:00
有效期至: 2121-11-03 15:39:36+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x543fd90b
哈希算法: sha256
证书MD5: 3b2c457ae92d080b8de339226ded16fc
证书SHA1: afa9b8102ed9249334e7dae69a3327dfbf9643bb
证书SHA256: 35762758ce86a6ec297d9ccac689469bc43b9fed8ae1b27f100a86bbac00a055
证书SHA512:
d2d4bee95bfd42d015cfef7d057e11a048793f51f5b2f8bdd4acdb57a0dc13a2c4be9e8b7d7a3fa61e69c95a4b11f3711386d0ed0f0f6a94af2b9a630cab72c0

公钥算法: rsa
密钥长度: 2048
指纹: 55e1b9518ad6710f1a975f68213f972512c387be4818f793ae105b221fb67880
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
moe.nb4a.SERVICE	未知	未知权限	来自 android 引用的未知权限。
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_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	普通	启用特殊用途的前台服务	允许常规应用程序使用类型为“specialUse”的 Service.startForeground。
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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。

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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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。
moe.nb4a.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
io.nekohasekai.sagernet.ui.MainActivity	Schemes: sn://, clash://, ss://, ssr://, socks://, socks4://, socksa://, socks5://, vmess://, trojan://, trojan-go://, naive+https://, naive+quic://, hysteria:// Hosts: subscription, install-config,

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: 1 | 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: 7 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息

1	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity (io.nekohasekai.sagernet.QuickToggleShortcut) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Service (io.nekohasekai.sagernet.bg.TileService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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。
5	Broadcast Receiver (io.nekohasekai.sagernet.BootReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
6	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_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。
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。
8	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: **6** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	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
5	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
6	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
7	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
8	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
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
00013	读取文件并将其放入流中	文件	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
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
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 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
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00026	方法反射	反射	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	4/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.CAMERA android.permission.VIBRATE
其它常用权限	8/46	android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE

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

matsuridayo.github.io	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.cloudflareclient.com	安全	否	**IP地址:** 104.17.143.163 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
dns.google	安全	否	**IP地址:** 185.199.108.153 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.386051 **经度:** -122.083847 **查看:** Google 地图
neko-box.pages.dev	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
cp.cloudflare.com	安全	否	**IP地址:** 104.17.143.163 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
yaml.org	安全	否	**IP地址:** 104.17.143.163 **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
f-droid.org	安全	否	**IP地址:** 185.199.108.153 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

unlicense.org	安全	否	**IP地址:** 104.21.5.81 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
t.me	安全	否	**IP地址:** 185.199.108.153 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 172.19.0.2 • 172.19.0.1	io/nekohasekai/sagernet/bg/VpnService.java
• https://yaml.org/spec/1.1/#id934537	org/yaml/snakeyaml/DumperOptions.java
• https://github.com/matsuridayo/nekoboxforandroid • https://github.com/matsuridayo/nekoboxforandroid/releases • https://matsuridayo.github.io/index_docs/#donate • https://t.me/matsuridayo	io/nekohasekai/sagernet/ui/AboutFragment.java
• https://matsuridayo.github.io/nb4a-route/	io/nekohasekai/sagernet/ui/RouteFragment.java
• https://matsuridayo.github.io/m-plugin/	io/nekohasekai/sagernet/ui/StunActivity$$ExternalSyntheticLambda0.java
• 127.0.0.1	io/nekohasekai/sagernet/fmt/naive/NaiveFmtKt.java
• https://api.cloudflareclient.com/v0a1922/reg/ • https://api.cloudflareclient.com/v0a1922/reg • https://api.cloudflareclient.com	io/nekohasekai/sagernet/utils/Cloudflare.java
• 127.0.0.	io/nekohasekai/sagernet/fmt/hysteria/HysteriaFmtKt.java
• https://matsuridayo.github.io/m-plugin/	io/nekohasekai/sagernet/ui/MainActivity$$ExternalSyntheticLambda7.java
• 127.0.0.1	io/nekohasekai/sagernet/fmt/ConfigBuilderKt.java
• http://cp.cloudflare.com/	io/nekohasekai/sagernet/ConstantsKt.java

• https://223.5.5.5/dns-query • https://dns.google/dns-query • http://127.0.0.1:9090/ui	io/nekohasekai/sagernet/database/DataStore.java
• https://github.com/matsuridayo/plugins/releases?q=hysteria • https://github.com/matsuridayo/plugins/releases?q=mieru • https://matsuridayo.github.io/ • https://github.com/matsuridayo/plugins/releases?q=naive	io/nekohasekai/sagernet/fmt/PluginEntry.java
• https://neko-box.pages.dev/喵 • https://play.google.com/store/apps/details?id= • https://matsuridayo.github.io/ • https://f-droid.org/packages/	io/nekohasekai/sagernet/ui/MainActivity.java
• 127.0.0.1 • https://unlicense.org	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Golang	Google	Go 是一种开源编程语言，可轻松构建简单，可靠和高效的软件。
Process Phoenix	JakeWharton	Process Phoenix facilitates restarting your application process.
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack ProfileInstaller	Google	此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).
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
"password" : "Password"
"route_bypass" : "Bypass"
"ssh_auth_type_none" : "None"
"username" : "Username"
"route_bypass" : "Bypass"
"ssh_auth_type_none" : "Kosong"

本报告由南明离火移动安全分析平台生成

"ssh_auth_type_none" : "Aucun"
"password" : "Parola"
"route_bypass" : "Atlat"
"route_bypass" : "Omitir"
"ssh_auth_type_none" : "Ninguna"
"hysteria_auth_payload" : "Identitetbekreftelses-nyttelast"
"hysteria_auth_type" : "Identitetbekreftelsestype"
"password" : "Passord"
"ssh_auth_type_none" : "Ingen"
"username" : "Brukernavn"
a79ada0ab5ab3b894f420add507b1e8f
1dbf667053726c13d139a4d83c41f895
f1aab1fb633378621635c344dbc8ac7b
b4884880479b3ec07ec5136206e4acfd

免责声明及风险提示: