南明离火
移动应用检测平台

ANDROID 静态分析报告

星辰VPN • v1.2.3

分析日期: 2025-08-29 13:35:34

应用概览

文件名称:	星辰VPN v1.2.3.apk
文件大小:	24.23MB
应用名称:	星辰VPN
软件包名:	com.moetor.freenetmt
主活动:	com.moetor.ui.BootActivity
版本号:	1.2.3
最小SDK:	21
目标SDK:	32
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	55/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	4ca3f4f5269d2a2c6d8a121d2d8fde70
SHA1:	8dd5d72cf133fb8c36a4b723199fc75ec27ae17a
SHA256:	811277d9b06eafe27d78d3293f1f00329ba5d8f51a05714a2d3843776a59f55

分析结果严重性分布

高危	中危	信息	安全	关注
1	13	3	2	0

四大组件导出状态统计

Activity组件：22个，其中export的有： 0个
Service组件：5个，其中export的有： 1个
Receiver组件：2个，其中export的有： 1个
Provider组件：7个，其中export的有： 1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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-22 06:22:21+00:00
有效期至: 2051-04-09 06:22:21+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x7b52b58f
哈希算法: sha256
证书MD5: 6cd05786806177a4e55d0b9f784b62ba
证书SHA1: 2712a037014a9a51effa4967440ab570d73bcf11
证书SHA256: c2ffc8209ae544facaaa92e8ae2848e2e1981715c9d46e44b9f1665a9b1e9d86
证书SHA512:
42cb835a8383b77c553c88cfc9752a152888a33d4a3ca01d992a3ebf4829b92c7299acdf3ad1286251ef23c88cf91fb80828adfc06a51c0f65c624abdbb02ce5

公钥算法: rsa
密钥长度: 2048
指纹: 06cecbcbab418e93ac4bced23e79c140091de4858831e30fe63d861d6bc8d578
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.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.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.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.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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
com.moetor.freenet.permission.RECEIVE_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
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.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。

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.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.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序

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: **4** | 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=@7F150003]	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	Service (com.moetor.app.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。
4	Broadcast Receiver (com.moetor.app.RestartReceiver) 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。

5	Content Provider (com.github.kr328.clash.service.FilesProvider) 受权限保护，但应检查权限保护级别。Permission: android.permission.MANAGE_DOCUMENTS [android:exported=true]	警告	检测到 Content Provider 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: **1** | 警告: **8** | 信息: **3** | 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	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
4	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
5	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	警告	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
6	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
7	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

8	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
9	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
10	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
11	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
12	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
13	MD5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 STRIPPED(裁剪符号表)
1	arm64-v8a/libbridge.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代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便对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。	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	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 warning 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	True info 符号被剥离

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
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
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
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
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
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
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
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
00029	动态初始化类对象	反射	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
00192	获取短信收件箱中的消息	短信	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.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	6/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET 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
donate.kr328.app	安全	否	No Geolocation information available.
q4.qlogo.cn	安全	是	**IP地址:** 27.155.118.96 **国家:** 中国 **地区:** 福建 **城市:** 福州市 **纬度:** 26.099774 **经度:** 119.302148 **查看:** 高德地图
icon-icons.com	安全	否	**IP地址:** 172.67.72.210 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
dashif.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
m.goudan.site	安全	否	**IP地址:** 159.13.55.14 **国家:** 澳大利亚 **地区:** 新南威尔士州 **城市:** 悉尼 **纬度:** -33.867779 **经度:** 151.207047 **查看:** Google 地图
flagicons.lipis.dev	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
settings.crisp.chat	安全	否	**IP地址:** 104.18.28.104 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

t.me	安全	否	**IP地址:** 149.154.167.99 **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
twitter.com	安全	否	**IP地址:** 104.18.28.104 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
telegram.me	安全	否	**IP地址:** 104.21.70.253 **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
image.crisp.chat	安全	否	**IP地址:** 104.18.28.104 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
crisp.chat	安全	否	**IP地址:** 104.21.70.253 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
www.dailymotion.com	安全	否	**IP地址:** 34.214.37.125 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
fdn.geekzu.org	安全	否	**IP地址:** 104.21.70.253 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://crisp.chat/en/ • https://www.google.com/	im/crisp/client/internal/u/b.java
• https://flagicons.lipis.dev/flags/4x3/%s.svg	com/moetor/utils/CountryKt.java
• https://telegram.me/ • https://twitter.com/	im/crisp/client/internal/c/a.java
• https://fdn.geekzu.org/avatar/ • https://q4.qlogo.cn/g?b=qq&nk=	com/moetor/app/ExtKt.java
• https://m.goudan.site	com/moetor/app/MV.java
• https://m.goudan.site/mt.json	com/moetor/ui/BootActivity.java
• www.dailymotion.com	im/crisp/client/internal/c/h.java
• https://m.goudan.site/mt.json	com/moetor/ui/mine/SettingActivity.java
• 172.19.0.1 • 172.19.0.2	com/github/kr328/clash/service/TunService.java
• https://github.com/lingochamp/filedownloader/wiki/filedownloader.properties	k3/a.java
• https://crisp.chat/	im/crisp/client/internal/j/b.java
• https://settings.crisp.chat/client/website/	im/crisp/client/internal/l/a.java
• https://image.crisp.chat/ • https://image.crisp.chat/avatar/website/ • https://image.crisp.chat/avatar/operator/	im/crisp/client/internal/k/a.java
• http://dashif.org/guidelines/trickmode • http://dashif.org/guidelines/last-segment-number	c2/d.java
• https://github.com/kr328/clashforandroid • https://icon-icons.com/downloadimage.php?id=89781&root=1368/png/512/&file=-avatar_89781.png • https://github.com/kr328/clashforandroid/issues • https://github.com/dreamacro/clash • https://donate.kr328.app • https://play.google.com/store/apps/details?id=com.github.kr328.clash • https://github.com/kr328/clashforandroid/releases • https://github.com/dreamacro/clash/wiki	自研引擎-S
• https://t.me/wallyperry	lib/arm64-v8a/libbridge.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Clash Core	Dreamacro	A rule-based tunnel in Go.

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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。
FileDownloader	LingoChamp	Android 文件下载引擎，稳定、高效、灵活、简单易用。

邮箱地址敏感信息提取

EMAIL	源码文件
name@site.ru	自研引擎-S

敏感凭证泄露检测

可能的密钥
08c06d320345bb682d17f10faa6f9e6f
344f4abf0a10cb27a43e94dd31b44900

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患。