南明离火
移动应用检测平台

ANDROID 静态分析报告

LightningX VPN • v3.0.5

分析日期: 2025-07-05 15:48:24

应用概览

文件名称:	base.apk
文件大小:	32.95MB
应用名称:	LightningX VPN
软件包名:	com.shanlian.pro
主活动:	com.sanlian.shanlian.MainActivity
版本号:	3.0.5
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	4/432
杀软检测:	AI评估：安全
MD5:	687681f215642be916b0d79ce1ec8865
SHA1:	9872636ef48e3be87a31528cb01fa6e2eaf1472
SHA256:	b1e542d2093d7e0a2b16fcfc00153429bfb2356f87f9e55919fe7b7d9cbb9ddb

分析结果严重性分布

高危	中危	信息	安全	关注
4	19	3	3	2

四大组件导出状态统计

Activity组件：17个，其中export的有： 1个
Service组件：16个，其中export的有： 1个
Receiver组件：9个，其中export的有： 4个

Provider组件：7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: CN=shanlian, OU=shanlian, O=shanlian, L=shanlian, ST=shanlian
签名算法: rsassa_pkcs1v15
有效期自: 2024-01-27 03:39:05+00:00
有效期至: 2049-01-20 03:39:05+00:00
发行人: CN=shanlian, OU=shanlian, O=shanlian, L=shanlian, ST=shanlian
序列号: 0x1
哈希算法: sha256
证书MD5: 68dc61f8b75560556a2fbba254f156ea
证书SHA1: b95e94c694606ec28964511c4fe328d4f5e36a47
证书SHA256: ca6dff51eff3a958f0a58a6fad5237b992c6454b179a5c4f091854c166f89fbe
证书SHA512:
bff2d2ac69c19fd6ccfc8ae3d4f1037e1f6921eafb0c15420cde9ff2368239f3434cea419ba8f5c787062feec35857dadc1e4300cc8381232bd7d30b02c5bcf

公钥算法: rsa
密钥长度: 2048
指纹: 2922409cb808c394bdbfdbd33ce0ba19ecea507011e15fe1388e8441c38324b5
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.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.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.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_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.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_US	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.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.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.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.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.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.REQUEST_COMPANION_RUN_IN_BACKGROUND	普通	允许配套应用程序在后台运行	允许配套应用在后台运行。
android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	普通	允许配套应用程序在后台使用数据	允许配套应用在后台使用数据。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.shanjian.pro.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT

com.sanlian.shanlian.MainActivity	Schemes: https://, Hosts: link.lightningxvpn.com,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.shanlian.pro,

网络通信安全风险分析

高危: **1** | 警告: **1** | 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。
2	*	警告	基本配置配置为信任系统证书。

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: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	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。
3	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。
4	Activity (com.facebook.CustomTabActivity) 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。
5	Service (com.applozic.mobicomkit.uiwidgets.KmFirebaseMessagingService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。

本报告由南明离火移动安全分析平台生成

6	Broadcast Receiver (com.applozic.mobicomkit.broadcast.TimeChangeBroadcastReceiver) 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。
7	Broadcast Receiver (com.applozic.mobicomkit.broadcast.ConnectivityReceiver) 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。
8	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
9	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: **3** | 警告: **8** | 信息: **3** | 安全: **2** | 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
3	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

4	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
5	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: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	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
7	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
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
9	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
10	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

11	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
12	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
13	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
14	该文件是World Writable。任何应用程序都可以写入文件	高危	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
15	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
16	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

应用行为分析

编号	行为	标签	文件
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
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
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

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
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
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	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
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
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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	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
00191	获取短信收件箱中的消息	短信	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
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
00121	创建目录	文件 命令	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
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00009	将游标中的数据放入 JSON 对象	文件	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.VIBRATE android.permission.WAKE_LOCK android.permission.CAMERA

本报告由南明离火移动安全分析平台生成

其它常用权限	13/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_NOTIFICATION_POLICY com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
socket-eu.kommunicate.io	安全	否	**IP地址:** 34.54.128.129 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
api-eu.kommunicate.io	安全	否	**IP地址:** 142.251.40.51 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
apps.applozic.com	安全	否	No Geolocation information available.
link.lightningxvpn.com	安全	否	**IP地址:** 104.26.1.149 **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

firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
graph-video.s	安全	否	No Geolocation information available.
chat-eu.kommunicate.io	安全	否	**IP地址:** 34.54.128.129 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
helpcenter.kommunicate.io	安全	否	**IP地址:** 3.163.125.92 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.176.14 **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
chat.kommunicate.io	安全	否	**IP地址:** 3.216.206.213 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
facebook.com	安全	否	**IP地址:** 31.13.70.36 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
journeyapps.com	安全	否	**IP地址:** 216.137.39.33 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

graph.s	安全	否	No Geolocation information available.
api.kommunicate.io	安全	否	**IP地址:** 3.218.9.89 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.mobitexter.net	安全	否	**IP地址:** 104.21.16.1 **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
socket.kommunicate.io	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://app-measurement.com/a	m6/j0.java
• https://firebase.google.com/docs/analytics	d6/u2.java
• https://facebook.com/device?user_code=%1$s&qr=1	m4/m.java
• https://github.com/flutter/packages/blob/master/packages/in_app_purchase/in_app_purchase/readme.md#loading-products-for-sale	gd/g0.java
• https://chat.kommunicate.io	com/applozic/mobicomkit/ALGroupInfoTask.java
• https://play.google.com/store/apps/details?id=	fc/d.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	f9/t.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	m9/f.java
• https://graph-video.%s • https://graph.%s	c4/i0.java
• https://firebase.google.com/support/privacy/init-options	y9/g.java
• https://helpcenter.kommunicate.io/ • https://helpcenter.kommunicate.io	io/kommunicate/services/KmUserClientService.java

• https://chat.kommunicate.io • tcp://socket.kommunicate.io:1883 • tcp://apps.applozic.com:1883 • https://api.kommunicate.io	com/applozic/mobicomkit/api/MobiComKitClientService.java
• https://%s/%s/%s	ba/c.java
• https://www.google.com • https://goo.gl/naoooi • www.google.com	n6/fd.java
• https://chat-eu.kommunicate.io • https://chat.kommunicate.io • https://api.kommunicate.io • tcp://socket-eu.kommunicate.io:1883 • https://api-eu.kommunicate.io • tcp://socket.kommunicate.io:1883	io/kommunicate/Kommunicate.java
• https://.facebook.com • https://facebook.com	c4/m0.java
• https://link.lightningxvpn.com	com/sanlian/shanlian/MainActivity.java
• https://app-measurement.com/a	d6/ce.java
• https://journeyapps.com/ • https://github.com/journeyapps/zxing-android-embedded • http://www.mobitexter.net/	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/332246665429/namespaces/firebase:fetch?key=AIzaSyD659kmLdLx4nwCA8TLF9HWQ6YyPfUEvig ） 已禁用响应体内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。

Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱地址敏感信息提取

EMAIL	源码文件
support@mobitexter.net	自研引擎-S

第三方追踪器检测

名称	类别	网址
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"delivery_report_pref_key" : "DELIVERY_REPORT_ENABLE"

"device_key_string" : "DEVICE_KEY_STRING"
"facebook_app_id" : "3542276252653495"
"facebook_client_token" : "2ad94a08e9755dbc0cdb396c929a40fd"
"google_api_key" : "AIzaSyD659kmLdLx4nwCA8TLF9HWQ6YyPfUEvig"
"google_app_id" : "1:332246665429:android:d97a9856fe50006f327a5c"
"google_crash_reporting_api_key" : "AIzaSyD659kmLdLx4nwCA8TLF9HWQ6YyPfUEvig"
"group_sms_freq_key" : "GROUP_SMS_FREQ_KEY"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"phone_number_key" : "phone_number_key"
"received_sms_sync_pref_key" : "RECEIVED_SMS_SYNC_FLAG"
"sent_sms_sync_pref_key" : "SENT_SMS_SYNC_FLAG"
"user_key_string" : "SU_USER_KEY_STRING"
"webhook_enable_key" : "WEBHOOK_ENABLE_KEY"
cc2751449a350f668590264ed76692694a80308a
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
VGhpcyBpcyB0aGUga2V5IGZvciBIHNlY3VyZZBzdG9yYWdlIEFFUyBLZXkK
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
9b8f518b086098de3d77736f9458a3d2f6f95a37
470fa2b4ae81cd56ecbcda9735803434cec591fa
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
c56fb7d591ba6704df047fd98f535372fea00211
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg

Google Play 应用市场信息

标题: 闪连VPN：超快无限VPN

评分: 4.234568 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.shanlian.pro

开发者信息: LightningX Team, 5658695376886984698, None, https://lightningxvpn.com/, support@lightningxvpn.com,

发布日期: 2024年2月27日 **隐私政策:** Privacy link

关于此应用:

闪连VPN（LightningX VPN）是一款快速、稳定且安全的VPN应用。具有一键连接、匿名上网、全面保护你的隐私和安全、无限浏览、无带宽或速度限制、零日志等特点。 主要特点： - 提供60多个国家的2000多个高速服务器。 - 无限流量、带宽和速度，速度达到600Mbps或更快。 - 保护您的在线隐私和安全，享受安全的线上浏览。 - 使用强大的加密协议和算法（WireGuard、Shadowsocks、Vless、AES-256）加密您的数据和流量。 - 严格遵循无日志政策，绝不存储浏览活动。 - 提供DNS和IP泄漏保护。 - 解锁和访问各种网站、平台或服务，如YouTube、TikTok、Netflix等。 - 在您的安卓手机、安卓TV、Windows、iPhone、iPad、Mac或Apple TV上享受稳定高速的互联网连接。 - 支持多个设备同时连接。 - 一键连接，直观易操作的界面。 - 支持9种语言，随时切换不同语言。 - 提供24/7全天候客户支持，通过实时聊天或电子邮件联系。 为什么使用LightningX VPN: 获取私人且安全的互联网连接，尤其是在公共网络中。 - 更改您的IP地址，以绕过地区限制，访问全球内容。 服务器位置列表： 闪连VPN提供60多个国家的服务器，包括以下国家： - 美国 - 加拿大 - 澳大利亚 - 英国 - 西班牙 - 法国 - 瑞士 - 意大利 - 奥地利 - 荷兰 - 德国 - 比利时 - 巴西 - 日本 - 新加坡 - 香港 - 印度 - 印度尼西亚 - 以及更多国家 计划与定价： 闪连VPN提供免费试用和适合每个用户的灵活套餐。免费下载并试用此VPN。支持应用内购买。您可以根据需要选择每周到每年的计划。 - 1个月计划：$8.99 - 1季度计划：$15.99 - 1年计划：$59.99 立即安装闪连VPN，您的终极互联网伴侣。体验超快的网速、全面的隐私保护、无限流量和带宽，以及专业的客户支持。马上开始使用这个VPN，享受安全、快速和无限制的互联网吧！ EULA: https://lightningxvpn.com/eula/

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隐患。