南明离火
移动应用检测平台

ANDROID 静态分析报告

黑洞加速器 • v5.17243.30718

分析日期: 2025-07-06 20:41:53

应用概览

文件名称:	黑洞加速器.apk
文件大小:	23.7MB
应用名称:	黑洞加速器
软件包名:	com.blackhole.hd1724530718
主活动:	com.blackhole.hd1724530718.ui.SplashActivity
版本号:	5.17245.30718
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	42/100 (中风险)
杀软检测:	2 个杀毒软件报毒
MD5:	a0a8b078e9bc6a17157e50fda3a67452
SHA1:	e6f8b8645956651528108c7830de0215bd07c791
SHA256:	bf67d6b17eb4af796c67144df4f386ef6b79697be2f5955aadd58d7b64ccf28

分析结果严重性分布

高危	中危	信息	安全	关注
5	17	2	1	4

四大组件导出状态统计

Activity组件：31个，其中export的有： 4个
Service组件：4个，其中export的有： 1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

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=1724530718, ST=1724530718, L=1724530718, O=1724530718, OU=1724530718, CN=1724530718
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-24 20:19:06+00:00
有效期至: 2034-08-22 20:19:06+00:00
发行人: C=1724530718, ST=1724530718, L=1724530718, O=1724530718, OU=1724530718, CN=1724530718
序列号: 0x36574720
哈希算法: sha256
证书MD5: 5ddda87e4923daa3e4f30ed3f2c686ca
证书SHA1: a5e8d6d1ccebdb21369428cbe9256ba30cdb012c
证书SHA256: 608ec2511ff3746c53eb7989417061084738f42c5e0adaa9f302929fb573ba14
证书SHA512:
72515b39f3d0cdba4a708bdd3bdf914cf7dca1f365119efc4f7b4b807f6dc68932c776b39d406d6789d538c8475089e66ca4b814de2cb162a79c8633270800a

公钥算法: rsa
密钥长度: 2048
指纹: f0bc0f943326a1597beb948b3ac458303e5c93009c64996968a630b683ad923a
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.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。
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.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。
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。
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_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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。

com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	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
com.ljoy.chatbot.FAQActivity	Schemes: https://, Hosts: cs30.net, Path Prefixes: /elvaFAQ,

网络通信安全风险分析

高危: **2** | 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。
3	*	高危	基本配置配置为信任用户安装的证书。

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: **1** | 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、Media Player 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	Activity (com.blackhole.hd1724530718.ui.MainActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

4	App 链接 assetlinks.json 文件未找到 [android:name=com.ljoy.chatbot.FAQActivity] [android:host=https://cs30.net]	高危	App Link 资产验证 URL（https://cs30.net/.well-known/assetlinks.json）未找到或配置不正确。（状态码：None）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
5	Activity (com.ljoy.chatbot.FAQActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
6	Activity (com.ljoy.chatbot.WebViewActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
7	Service (com.blackhole.hd1724530718.service.QSTileService) 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。
8	Activity (com.blackhole.hd1724530718.ui.TaskerActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
9	Broadcast Receiver (com.blackhole.hd1724530718.receiver.TaskerReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。Intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。

代码安全漏洞检测

高危: **2** | 警告: **8** | 信息: **2** | 安全: **0** | 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,不应记录敏感信息	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

本报告由南明离火移动安全分析平台生成

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	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	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
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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	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
9	IP地址泄漏	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
10	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

11	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
12	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

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
00091	从广播中检索数据	信息收集	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
00012	读取数据并放入缓冲流	文件	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
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
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
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
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
00192	获取短信收件箱中的消息	短信	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
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
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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限

00065	获取SIM卡提供商的国家代码	信息收集	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
00035	查询已安装的包列表	反射	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
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
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
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
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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
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
00028	从assets目录中读取文件	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
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
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00032	加载给定类	反射	升级会员：解锁高级权限
00046	方法反射	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	3/30	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.WRITE_SETTINGS

其它常用权限	6/46	android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE 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
cdn.aihelp.net	安全	否	**IP地址:** 43.129.21.104 **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
www.h7sq4d.xyz	安全	否	No Geolocation information available.
www.hhkbdd.xyz	安全	否	No Geolocation information available.
proxy.aihelp.net	安全	是	**IP地址:** 43.129.21.104 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
pv.sohu.com	安全	是	**IP地址:** 43.129.21.104 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
www.hkeild.xyz	安全	否	No Geolocation information available.
1.2345345.xyz	安全	否	**IP地址:** 172.67.190.50 **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

aihelp.net	安全	是	IP地址: 43.129.21.104 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图
cs30.net	安全	是	IP地址: 1.14.224.97 国家: 中国 地区: 广东 城市: 广州 纬度: 23.127361 经度: 113.264572 查看: 高德地图
www.hicv2d.xyz	安全	否	No Geolocation information available.
raw.githubusercontent.com	安全	否	IP地址: 185.199.111.133 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
www.h28334d.xyz	安全	否	No Geolocation information available.
www.h58205d.xyz	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• tcp://127.0.0.1:1883	org/fusesource/mqtt/client/MQTT.java
• https://play.google.com/store/apps/details?id=	com/ljoy/chatbot/sdk/ELvaChatServiceSdk.java
• www.google.com • 127.0.0.1	com/blackhole/hd1724530718/util/Utils.java
• 127.0.0.1	com/blackhole/hd1724530718/util/V2rayConfigUtil.java
• https://github.com/2dust/v2rayng/issues • https://1.2345345.xyz/ads.html • https://raw.githubusercontent.com/2dust/androidpackagenamelist/master/proxy.txt • 1.1.1.1 • 223.5.5.5 • https://raw.githubusercontent.com/2dust/v2raycustomroutinglist/master/	com/blackhole/hd1724530718/AppConfig.java

• http://cs30.net/elva/api/init • http://%s/elva/api/init	com/ljoy/chatbot/core/sfsapi/SendRequestTask.java
• file:下载完成 • file:删除faq旧文件成功! • file:删除story旧文件成功!	com/ljoy/chatbot/utils/ABDownloadUtil.java
• https://aihelp.net/forum/? • https://aihelp.net/forum/home/index/bestlist/?	com/ljoy/chatbot/QAWebActivity.java
• http://pv.sohu.com/cityjson?ie=utf-8	com/ljoy/chatbot/utils/DeviceLocalInfoService.java
• https://www.h7sq4d.xyz:20000 • https://www.hicv2d.xyz:20000 • https://www.hkejld.xyz:20000 • https://www.h58205d.xyz:20000 • https://www.h28334d.xyz:20000 • https://www.hhkbdd.xyz:20000	com/blackhole/hd1724530718/ui/CommUiApiKt.java
• https://play.google.com/store/apps/details?id=	com/ljoy/chatbot/utils/ABMobileUtil.java

• https://cs30.net/elva/api/faqs2 • https://proxy.aihelp.net/forum/home/index/bestlist • https://proxy.aihelp.net/elva/api/faqs2 • https://cs30.net/elva/api/faqs1 • https://aihelp.net/forum • http://cs30.net/elva/api/init • https://aihelp.net/elva/api/crmtoken • http://cs30.net/elva/api/initset • https://cs30.net/elva/api/initset • https://cs30.net/elva/api/vipinfo • https://cs30.net/elva/api/init • http://proxy.aihelp.net/elva/api/initset • 169.44.24.184 • https://proxy.aihelp.net/forum • https://proxy.aihelp.net/elva/api/initset • https://cdn.aihelp.net/elva • https://cs30.net/elva/api/initget • 169.44.24.179 • https://aihelp.net/elva/mfaq/show.aspx • https://proxy.aihelp.net/elva/api/init • https://proxy.aihelp.net/elva/api/faqs • https://proxy.aihelp.net/elva/api/point • https://proxy.aihelp.net/elva/api/faqs1 • https://aihelp.net/forum/home/index/bestlist • https://cs30.net/elva/api/point • https://proxy.aihelp.net/fileservice/api/upload • https://proxy.aihelp.net/elva/mfaq/show.aspx • https://cs30.net/elva/api/faqs • http://aihelp.net/elva/api/crmtoken • https://aihelp.net/elva/api/elvaapi	com/joy/chatbot/utils/Constants.java

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。

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。

邮箱地址敏感信息提取

EMAIL	源码文件
heidong2025@gmail.com	com/blackhole/hd1724530718/ui/MainActivity.java

敏感凭证泄露检测

可能的密钥
de18e79e-d0e2-41fe-b99e-7bd3b8950ca6
9dba66dd81324f8f8ef81527344037e2
954d976c3c9fd5e5c63dab4016cc12da
e0bc91b2-4eb0-4550-8764-925fb66a6185
a3482e88-686a-4a58-8126-99c9df64b7bf

免责声明及风险提示: