南明离火
移动应用检测平台

ANDROID 静态分析报告

Max OpenVPN • v1.0.5

分析日期: 2025-06-20 20:59:27

应用概览

文件名称:	f43bb262ab6c21a1b570174f3b11f3616cfcaacf51afdd37047a7dae3e0cc36e.apk
文件大小:	7.21MB
应用名称:	Max OpenVPN
软件包名:	com.dev.openvpn
主活动:	net.openvpn.openvpn.OpenVPNClient
版本号:	1.0.5
最小SDK:	21
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	47/100 (中风险)
杀软检测:	9 个杀毒软件报毒
MD5:	ff1c54ad571511b9ee377201bfb3c6c5
SHA1:	d4c0dca893d9c5b0b7b1c70bfaa5911765af263b
SHA256:	f43bb262ab6c21a1b570174f3b11f3616cfcaacf51afdd37047a7dae3e0cc36e

分析结果严重性分布

高危	中危	信息	安全	关注
2	1	2	1	0

四大组件导出状态统计

Activity组件：26个，其中export的有： 5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：0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
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772721f7958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

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.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	查看网络状态	允许应用程序查看所有网络的状态。
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
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.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.VIBRATE	普通	控制振动器	允许应用程序控制振动器。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。

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）

可浏览 Activity 组件分析

ACTIVITY	INTENT
net.openvpn.openvpn.OpenVPNAttachmentReceiver	Schemes: file://, Hosts: *, Mime Types: application/x-openvpn-profile, Path Patterns: .*\\.ovpn,

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	应用程序使用代码签名证书签名
易受 Janus 漏洞影响的应用程序	警告	应用程序使用 v1 签名方案签名，如果仅使用 v1 签名方案签名，则使其容易受到 Android 5.0-8.0 上的 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: **1** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在一个有漏洞的安卓版本上 [minSdk=21]	警告	这个应用程序可以安装在一个有多个未修复漏洞的旧版本的安卓上。建议使用安卓系统8.0以上版本, API级别大于26 以获得合理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	高危	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Service (net.openvpn.openvpn.OpenVPNService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_VPN_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

5	Activity (net.openvpn.openvpn.Main) 未被保护。 存在一个intent-filter。	警告	发现一个n Activity被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Broadcast Receiver (net.openvpn.openvpn.OpenVPNRebootReceiver) 未被保护。 存在一个intent-filter。	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
7	Activity (net.openvpn.openvpn.OpenVPNAttachmentReceiver) 未被保护。 存在一个intent-filter。	警告	发现一个n Activity被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
8	Activity (net.openvpn.openvpn.AppScreen) 未被保护。 存在一个intent-filter。	警告	发现一个n Activity被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
9	Activity (net.openvpn.openvpn.panel.Login) 未被保护。 存在一个intent-filter。	警告	发现一个n Activity被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

代码安全漏洞检测

高危: **1** | 警告: **2** | 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,不得记录敏感信息。	信息	CWE: CWE-532: Insertion of Sensitive Information Into Log File OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
3	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

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: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	应用程序使用不安全的随机数生成器。	警告	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	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/libovpncli.so	True info NX标志位已启用，这标志着内存页不可执行，使得攻击者注入的shellcode代码不可执行。		False high 这个共享对象在栈上没有添加栈哨兵值。栈哨兵用于检测和防止利用覆盖返回地址。使用选项-fstack-protector-all来启用栈哨兵。		None info 共享对象没有设置运行时搜索路径或RPATH。	None info 共享对象未设置RUNPATH。	False warning 共享对象没有任何加强的函数。加强的函数提供了针对glibc的常见不安全函数（如strcpy，gets等）的缓冲区溢出检查。使用编译器选项-D_FORTIFY_SOURCE=2来加强函数。	True info 符号被去除。

2	armeabi-v7a/libovpncli.so	True info NX标志位已启用，这标志着内存页不可执行，使得攻击者注入的shellcode代码不可执行。		False high 这个共享对象在栈上没有添加栈哨兵值。栈哨兵用于检测和防止利用覆盖返回地址。使用选项-fstack-protector-all来启用栈哨兵。		None info 共享对象没有设置运行时搜索路径或RPATH。	None info 共享对象未设置RUNPATH。	False warning 共享对象没有任何加强的函数。加强的函数提供了针对glibc的常见不安全函数（如strcpy，gets等）的缓冲区溢出检查。使用编译器选项-D_FORTIFY_SOURCE=2来加强函数。	True info 符号被去除。
3	x86/libovpncli.so	True info NX标志位已启用，这标志着内存页不可执行，使得攻击者注入的shellcode代码不可执行。		True info 这个共享对象在栈上添加了一个栈哨兵值，这样当一个栈缓冲区溢出覆盖返回地址时，它也会被覆盖。这样可以通过在函数返回前验证哨兵的完整性来检测溢出。		None info 共享对象没有设置运行时搜索路径或RPATH。	None info 共享对象未设置RUNPATH。	False warning 共享对象没有任何加强的函数。加强的函数提供了针对glibc的常见不安全函数（如strcpy，gets等）的缓冲区溢出检查。使用编译器选项-D_FORTIFY_SOURCE=2来加强函数。	True info 符号被去除。
4	x86_64/libovpncli.so	True info NX标志位已启用，这标志着内存页不可执行，使得攻击者注入的shellcode代码不可执行。		False high 这个共享对象在栈上没有添加栈哨兵值。栈哨兵用于检测和防止利用覆盖返回地址。使用选项-fstack-protector-all来启用栈哨兵。		None info 共享对象没有设置运行时搜索路径或RPATH。	None info 共享对象未设置RUNPATH。	False warning 共享对象没有任何加强的函数。加强的函数提供了针对glibc的常见不安全函数（如strcpy，gets等）的缓冲区溢出检查。使用编译器选项-D_FORTIFY_SOURCE=2来加强函数。	True info 符号被去除。

恶意域名威胁检测

域名	状态	中国境内	位置信息

www.privatetunnel.com	安全	否	**IP地址:** 104.16.240.94 国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看: Google 地图
forums.openvpn.net	安全	否	**IP地址:** 3.72.228.171 国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110883 经度: 8.681995 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
• www.privatetunnel.com/index.php/profiledownload.html • www.privatetunnel.com/	自研引擎分析结果
• 8.8.8.8 • 8.8.4.4 • https://forums.openvpn.net/viewtopic.php?f=36&t=21873 • 255.255.255.252	lib/arm64-v8a/libovpncli.so
• 8.8.8.8 • 8.8.4.4 • https://forums.openvpn.net/viewtopic.php?f=36&t=21873 • 255.255.255.252	lib/armeabi-v7a/libovpncli.so
• 8.8.8.8 • 8.8.4.4 • 255.255.255.252 • https://forums.openvpn.net/viewtopic.php?f=36&t=21873	lib/x86/libovpncli.so
• 8.8.8.8 • 8.8.4.4 • https://forums.openvpn.net/viewtopic.php?f=36&t=21873 • 255.255.255.252	lib/x86_64/libovpncli.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Uses-Library-0	无	

免责声明及风险提示:

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。