南明离火
移动应用检测平台

ANDROID 静态分析报告

Shadowsocks • v5.3.4

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-14 22:24:36

应用概览

文件名称:	shadowsocks--universal-5.3.4.apk
文件大小:	24.34MB
应用名称:	Shadowsocks
软件包名:	com.github.shadowsocks
主活动:	com.github.shadowsocks.MainActivity
版本号:	5.3.4
最小SDK:	23
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:	54/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	8059b683e5d66e8a8ca18bc3fad115cf
SHA1:	fb717b106a136924ed65[illegible]ed76597460edde6ad12
SHA256:	386e463f5d283f0[illegible]3ff473775995d417867[illegible]9c15f896a079f868e4

分析结果严重性分布

高危	中危	信息	安全	关注
0	16	2	1	0

四大组件导出状态统计

Activity组件：12个，其中export的有： 4个
Service组件：18个，其中export的有： 2个
Receiver组件：13个，其中export的有： 4个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=cn, ST=Shanghai, L=Pudong, O=Fudan Univ., OU=PPI, CN=Max Lv
签名算法: rsassa_pkcs1v15
有效期自: 2011-02-19 05:00:54+00:00
有效期至: 2036-02-13 05:00:54+00:00
发行人: C=cn, ST=Shanghai, L=Pudong, O=Fudan Univ., OU=PPI, CN=Max Lv
序列号: 0x4d5f4e86
哈希算法: sha1
证书MD5: 2fd4c584fba42f6b45d23bd111bcc3e6
证书SHA1: 58a90f84cfe99d4280aec677c9a1292fae131677
证书SHA256: 92416ea4166422613d3d1d585ac1c70f0383407077134636b4cfb2f0bd8e01f0
证书SHA512:
db9dfaee244215923ce0621575078ad17e2363745611fb7b02cac6ae2b0d4ba8b29ece6f084607a9fcd06c25645237cc6b1e62e1b5583737beaa4fba05c02a52

公钥算法: rsa
密钥长度: 1024
指纹: 7d2d19ccce0442538941c41c47eb36e7295c1f608735f55072a4fccafbf96696
找到 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.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.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.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	普通	允许系统豁免类型的前台服务	允许常规应用程序使用类型为“systemExempted”的 Service.startForeground。仅允许应用程序在 ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED 中列出的用例中使用此类型。
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.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.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.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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。
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。
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.github.shadowsocks.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
com.github.shadowsocks.UrlImportActivity	Schemes: ss://,

网络通信安全风险分析

高危: **0** | 警告: **0** | 信息: **0** | 安全: **1**

序号	范围	严重级别	描述
1	*	安全	基本配置配置为禁止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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

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

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

3	Activity (com.github.shadowsocks.ScannerActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (com.github.shadowsocks.tasker.ConfigActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (com.github.shadowsocks.QuickToggleShortcut) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Service (com.github.shadowsocks.bg.TileService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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。
7	Broadcast Receiver (com.github.shadowsocks.tasker.ActionListener) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity (com.github.shadowsocks.UrlImportActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Broadcast Receiver (com.github.shadowsocks.BootReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_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。
11	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	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。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。
12	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	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。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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **0** | 警告: **2** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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

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）

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

1	arm64-v8a/libredsocks.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。	地址无关的可执行文件 (PIE) 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，以便它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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__vsprintf_chk', '__strlen_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk']	True info 符号被剥离
2	arm64-v8a/libsslocal.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。	地址无关的可执行文件 (PIE) 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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种方法。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	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
00121	创建目录	文件 命令	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
本报告由南明离火移动安全分析平台生成

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
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
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
00013	读取文件并将其放入流中	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	3/30	android.permission.CAMERA android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
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.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID 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
cp.cloudflare.com	安全	否	**IP地址:** 104.16.132.229 **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
docs.rs	安全	否	**IP地址:** 108.138.159.96 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.783058 **经度:** -96.806503 **查看:** Google 地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

shadowsocks.org	安全	否	**IP地址:** 104.21.10.62 **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
detectportal.firefox.com	安全	否	**IP地址:** 34.107.221.82 **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
admob-app-id-3330146721.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **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

URL 链接安全分析

URL信息	源码文件
• https://github.com/gfwlist/gfwlist/blob/master/gfwlist.txt	自研引擎-A
• https://cp.cloudflare.com	com/github/shadowsocks/net/HttpsTest.java
• 127.0.0.1	com/github/shadowsocks/preference/DataStore.java
• 127.0.0.1 • 172.19.0.2 • 172.19.0.1	com/github/shadowsocks/bg/VpnService.java
• 127.0.0.1	com/github/shadowsocks/bg/TransproxyService.java
• https://admob-app-id-3330146721.firebaseio.com • https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.ru.md • https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.md	自研引擎-S
• https://shadowsocks.org • https://github.com/shadowsocks/shadowsocks-org/issues/36 • 8.8.8.8 • data::optlengthcollectedhickory_proto::rr::record_dataevent • http://detectportal.firefox.com/success.txt • https://docs.rs/getrandom#nodejs-es-module-support/dev/urandom	lib/arm64-v8a/libsslocal.so

Firebase 配置安全检测

本报告由南明离火移动安全分析平台生成

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://admob-app-id-3330146721.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/261400168171/namespaces/firebase:fetch?key=AIzaSyCee3fAad7nb3YsxeUO9mqqHFfAvsSCbVs ） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		
		{
		"entries": {
		"proxy_url": "https://socks123.cdn.lol/get.php"
		},
		"state": "UPDATE",
		"templateVersion": "6"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
BarHopper	Google	BarHopper 是一个 ML Kit 中的库，用于在 Android 设备上识别或解码条形码。
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
Tun2Socks	Jason Lyu（xjasonlyu）	Tun2Socks 是一个网络通信库，它可以处理来自当前设备的任意应用的所有网络流量，并通过 HTTP/Socks4/Socks5/Shadowsocks 远程连接，支持 Windows、macOS 等多平台，并且支持 IPv6，可以提供最佳的性能。
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。
Open Source Notices	Google	Google Play 服务提供了一套工具，旨在让开发者更轻松地表达其应用中所用库的开源软件通知。其中一个工具就是 Gradle 插件，按照 POM 文件中的声明从包含的库收集许可条款，并创建可用于显示这些条款的 activity。
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。
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。
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。
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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

第三方追踪器检测

名称	类别	网址
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
凭证信息=> "com.google.android.backup.api_key" : "AEdPqrEAAAAI_zVxZthz2HDuz9toTvkYvL0L5GA-OjeUIfBeXg"
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-3283768469187309~3571758745"
"firebase_database_url" : "https://admob-app-id-3330146721.firebaseio.com"
"google_app_id" : "1:261400168171:android:dbdd6331c434162f"
"sitekey" : "Password"
"google_api_key" : "AIzaSyCee3fAad7nb3YsxeUO9mqqHFfAvsSCbVs"
"google_crash_reporting_api_key" : "AIzaSyCee3fAad7nb3YsxeUO9mqqHFfAvsSCbVs"
"sitekey" : "Passwort"
"com.google.firebase.crashlytics.mapping_file_id" : "aa06bd308ba6[illegible]f996638620a2cef333"
a79ada0ab5ab3b894f420add507b1e8f
5b5c55a1277c63e14416316f9198ed43
94a7fe8226719d48c1ec5aa5a851976f
f1aab1fb633378621635c344dbc8ac7b

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。

© 2025 南明离火 - 移动安全分析平台自动生成