南明离火
移动应用检测平台

ANDROID 静态分析报告

NetGuard • v2.234

分析日期: 2025-11-21 19:46:54

应用概览

文件名称:	NetGuard v2.334.apk
文件大小:	3.03MB
应用名称:	NetGuard
软件包名:	eu.faircode.netguard
主活动:	eu.faircode.netguard.ActivityMain
版本号:	2.334
最小SDK:	22
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:	53/100 (中风险)
杀软检测:	1 个杀毒软件报毒
MD5:	c9383bce497d2004d01955be7f3f5683
SHA1:	8ee4415789ed5d5e25093cc6d38f7b396e61e95b
SHA256:	300624ad3dea47af580f6262e41980cd55ab8d80ae009294ac99ee6ec4190e85

分析结果严重性分布

高危	中危	信息	安全	关注
0	0	2	1	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 2个
Service组件：8个，其中export的有： 6个
Receiver组件：6个，其中export的有： 4个
Provider组件：1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=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
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272c17958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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.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。
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.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.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.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.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.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。
eu.faircode.netguard.permission.ADMIN	未知	未知权限	来自 android 引用的未知权限。
eu.faircode.netguard.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全分析

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: **13** | 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=@7F130001]	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	Activity (eu.faircode.netguard.ActivitySettings) 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。
3	Activity (eu.faircode.netguard.ActivityForwardApproval) 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。
4	Service (eu.faircode.netguard.ServiceSinkhole) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_VPN_SERVICE [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。
5	Service (eu.faircode.netguard.ServiceExternal) 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。
6	Service (eu.faircode.netguard.ServiceTileMain) 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。

7	Service (eu.faircode.netguard.ServiceTileGraph) 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	Service (eu.faircode.netguard.ServiceTileFilter) 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。
9	Service (eu.faircode.netguard.ServiceTileLockdown) 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。
10	Broadcast Receiver (eu.faircode.netguard.ReceiverAutostart) 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。
11	Broadcast Receiver (eu.faircode.netguard.ReceiverPackageRemoved) 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。
12	Broadcast Receiver (eu.faircode.netguard.WidgetMain) 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。
13	Broadcast Receiver (eu.faircode.netguard.WidgetLockdown) 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。
14	Broadcast Receiver (eu.faircode.netguard.WidgetAdmin) 受权限保护。 Permission: eu.faircode.netguard.permission.ADMIN protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
15	高优先级 Intent（999） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **0** | 警告: **6** | 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: 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	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
4	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
5	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
6	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
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	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

应用行为分析

编号	行为	标签	文件

本报告由南明离火移动安全分析平台生成

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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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
00191	获取短信收件箱中的消息	短信	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
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
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
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
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
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
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
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
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
00023	从当前应用程序启动另一个应用程序	反射 控制	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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
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
00132	查询ISO国家代码	电话服务 信息收集	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.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.VIBRATE
其它常用权限	4/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.FOREGROUND_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
www.dnslytics.com	安全	否	**IP地址:** 188.114.96.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图
www.speedguide.net	安全	否	**IP地址:** 188.114.96.0 **国家:** 美国 **地区:** 佛罗里达州 **城市:** 杰克逊维尔 **纬度:** 30.332134 **经度:** -81.655670 **查看:** Google 地图
contact.faircode.eu	安全	否	**IP地址:** 99.86.240.49 **国家:** 奥地利 **地区:** Wien **城市:** 维也纳 **纬度:** 48.208889 **经度:** 16.372080 **查看:** Google 地图
www.netguard.me	安全	否	**IP地址:** 99.86.240.104 **国家:** 奥地利 **地区:** Wien **城市:** 维也纳 **纬度:** 48.208889 **经度:** 16.372080 **查看:** Google 地图

ipinfo.io	安全	否	**IP地址:** 34.117.59.81 **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
urlhaus.abuse.ch	安全	否	**IP地址:** 151.101.2.49 **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
• 10.1.10.1	eu/faircode/netguard/AdapterLog.java
• 127.0.0.1	eu/faircode/netguard/ActivityForwardApproval.java
• https://ipinfo.io/	eu/faircode/netguard/Util.java
• https://www.netguard.me/hosts • www.google.com • 10.1.10.1	eu/faircode/netguard/ActivitySettings.java
• http://www.netguard.me/#	eu/faircode/netguard/ActivityPro.java
• 10.1.10.1 • 8.8.8.8 • www.google.com • 255.255.255.255 • 255.255.255.254 • 8.8.4.4	eu/faircode/netguard/ServiceSinkhole.java
• https://www.netguard.me/hosts	eu/faircode/netguard/ServiceExternal.java
• https://contact.faircode.eu/?product=netguardstandalone • https://play.google.com/store/apps/details?id= • https://github.com/M66B/netguard/blob/master/faq.md • https://play.google.com/store/apps/dev?id=8420080860664580239 • https://www.netguard.me/ • https://urlhaus.abuse.ch/downloads/hostfile/	eu/faircode/netguard/ActivityMain.java
• https://github.com/M66B/netguard/blob/master/faq.md#user-content-faq27 • https://www.dnslytics.com/whois-lookup/ • 10.1.10.1 • https://www.speedguide.net/port.php?port=	eu/faircode/netguard/ActivityLog.java
• https://www.dnslytics.com/whois-lookup/ • https://www.speedguide.net/port.php?port=	eu/faircode/netguard/AdapterRule.java

本报告由南明离火移动安全分析平台生成

• https://contact.faircode.eu/?product=netguardstandalone • 255.255.255.255 • http://www.netguard.me/# • https://play.google.com/store/apps/details?id= • 127.0.0.1 • 10.1.10.1 • https://github.com/m66b/netguard/blob/master/faq.md#user-content-faq27 • https://ipinfo.io/ • https://www.netguard.me/hosts • www.google.com • https://urlhaus.abuse.ch/downloads/hostfile/ • 255.255.255.254 • https://www.speedguide.net/port.php?port= • https://play.google.com/store/apps/dev?id=8420080860664580239 • https://github.com/m66b/netguard/blob/master/faq.md • 8.8.8.8 • https://www.netguard.me/ • https://www.dnslytics.com/whois-lookup/ • 8.8.4.4	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
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程序启动时间。
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。

敏感凭证泄露检测

可能的密钥
dhP3Rfh[illegible]w9MEEKJLE8JwfRuSfSH0ZKYmUfsb86hCjjwYCaHHfqB0vUIB
FJsDEZ08LyD2sycgEA0F9pTi7Sjhe3xgGY
nk9RyZcJSaGcVgXXvK13YrDdGlmuEOr1iltGs3hWNatjJ41W0KTC
eyJhdWQiOiJUQVpP[illegible]1FMuLIsImV4cCI6MTg0MzE1ODcxNywiaWF0Ijo5NDM5MTQ3OTI1LCJpc3MiOiliLCJqdGkiOiliLCJuYmYiOjAsInN1YiI6IjIxNzEwNjU2MDMiLCJ0eXBlIjoiY[illegible]
nF8fMHi[illegible]vCrxXjHD6cY7tM87wHubuabpQgpVA==
mwWWSFaZ29ZxlAQk5JsrN606Q4HHMTssVuIq3sT

Google Play 应用市场信息

标题: NetGuard - no-root firewall

评分: None **安装:** 10,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** eu.faircode.netguard

开发者信息: Marcel Bokhorst, FairCode BV, 8420080860664580239, None, https://www.netguard.me/, marcel+help@faircode.eu,

发布日期: 2017年9月22日 **隐私政策:** Privacy link

关于此应用:

NetGuard 是一款互联网安全应用程序，它提供了简单而高级的方法来限制应用程序对互联网的访问。 可以单独允许或拒绝应用程序和地址访问您的 Wi-Fi 和/或移动连接。不需要 root 权限。 阻止对互联网的访问可以帮助： ＆公牛;减少您的数据使用量 ＆公牛;节省电池 ＆公牛;增加您的隐私 特征： ＆公牛;使用简单 ＆公牛;无需root ＆公牛; 100% 开源 ＆公牛;不打电话回家 ＆公牛;没有跟踪或分析 ＆公牛;无广告 ＆公牛;积极开发和支持 ＆公牛;支持Android 5.1及更高版本 ＆公牛;支持 IPv4/IPv6 TCP/UDP ＆公牛;支持网络共享 ＆公牛;屏幕打开时可选择允许 ＆公牛;漫游时可选择阻止 ＆公牛;可选择阻止系统应用程序 ＆公牛;可选择在应用程序访问互联网时发出通知 ＆公牛;可选择记录每个地址每个应用程序的网络使用情况 ＆公牛;材质设计主题有浅色和深色主题 专业版特点： ＆公牛;记录所有传出流量；搜索和过滤访问尝试；导出 PCAP 文件以分析流量 ＆公牛;允许/阻止每个应用程序的单独地址 ＆公牛;新应用通知；直接从通知配置 NetGuard ＆公牛;在状态栏通知中显示网络速度图 ＆公牛;从浅色和深色版本的五个附加主题中进行选择 没有其他无根防火墙可以提供所有这些功能。 如果您想测试新功能，可以参加测试计划：https://play.google.com/apps/testing/eu.faircode.netguard 此处描述了所有必需的权限：https://github.com/M66B/NetGuard/blob/master/FAQ.md#user-content-faq42 NetGuard 使用 Android VPNService 将流量路由到自身，因此可以在设备上而不是在服务器上过滤流量。只有一个应用程序可以同时使用此服务，这是 Android 的限制。 完整的源代码可以在这里找到：https://github.com/M66B/NetGuard

免责声明及风险提示: