南明离火
移动应用检测平台

ANDROID 静态分析报告

WroldPass Free VPN • v2.0.3

分析日期: 2024-03-25 16:05:17

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

应用概览

文件名称:	小三VPN_2.0.3.apk
文件大小:	9.28MB
应用名称:	WroldPass Free VPN
软件包名:	org.vpndigger
主活动:	com.worldpass.app.vpn.MainActivity
版本号:	2.0.3
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	a0f41ee97c0f84f39f29d3a80e386a29
SHA1:	4fc97c15e12bcb59b2dcc3de5263e515c44fd5ef
SHA256:	0a013f4209c5efb2e592c[illegible]70890d20450e[illegible]f8ba86ef6361f9249

分析结果严重性分布

高危	中等	信息	安全	关注
1	14	2	0	0

四大组件导出状态统计

Activity组件：16个，其中export的有：3个
Service组件：7个，其中export的有：1个
Receiver组件：3个，其中export的有：2个
Provider组件：6个，其中export的有：1个

应用签名证书信息

二进制文件已签名
v1 签名: True

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

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=MY, L=Kuala Lumpur, O=VPFree ORG, OU=TG, CN=vpfree
签名算法: rsassa_pkcs1v15
有效期自: 2020-08-14 01:41:05+00:00
有效期至: 2045-08-08 01:41:05+00:00
发行人: C=MY, L=Kuala Lumpur, O=VPFree ORG, OU=TG, CN=vpfree
序列号: 0x53a150f1
哈希算法: sha256
证书MD5: e8c3f87d6ce937bb3f879e1d70a5e26c
证书SHA1: e3f6d678e1f30c6c674cd30322d7da38418032cb
证书SHA256: 879905e69cf4fbc698ac932e74f6125552db8168282889362d2e9c7bee013a7f
证书SHA512:
106c6ae868c65ecf166fdc11c1e8a49eb5abb4e0dcf707c68ecc20e5939020bd713c9ad9de73eabe74294a50485052820e698adde627f6d8de67665b67689058

公钥算法: rsa
密钥长度: 2048
指纹: c23319eca372c765303156d5eeb956fa89194b48f03012d1c1c5b0a4592772b0
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.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.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_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.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.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。
org.vpndigger.permission.RECEIVE_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.worldpass.app.vpn.ExternalImportActivity	Schemes: clash://, Hosts: install-config,

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

com.microsoft.appcenter.distribute.DeepLinkActivity	Schemes: appcenter://, Hosts: updates, Paths: /,

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	*	警告	基本配置配置为信任系统证书。
2	*	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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

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	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
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	Activity (com.worldpass.app.vpn.ExternalImportActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
5	Service (com.worldpass.app.vpn.FileService) 受权限保护，但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。

本报告由南明离火移动安全分析平台生成

6	Broadcast Receiver (com.worldpass.app.vpn.RestartReceiver) 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，因此使其对设备上的任何其他应用程序都可访问。
7	Activity (com.microsoft.appcenter.distribute.DeepLinkActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
8	Broadcast Receiver (com.microsoft.appcenter.distribute.DownloadManagerReceiver) 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，因此使其对设备上的任何其他应用程序都可访问。
9	Content Provider (com.worldpass.app.vpn.service.FilesProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.MANAGE_DOCUMENTS [android:exported=true]	警告	发现一个 Content Provider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。

代码安全漏洞检测

高危: **0** | 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: 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
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，以便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

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

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	armeabi-v7a/libbridge.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 shell code 不可执行。		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	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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	6/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET 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。

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

恶意域名威胁检测

域名	状态	中国境内	位置信息
donate.kr328.app	安全	否	No Geolocation information available.
raw.githubusercontent.com	安全	否	**IP地址:** 185.199.108.133 **国家:** United States of America **地区:** Pennsylvania **城市:** California **纬度:** 40.065632 **经度:** -79.891708 **查看:** Google 地图
xoyondo.com	安全	否	**IP地址:** 104.26.3.171 **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
cdn.jsdelivr.net	安全	否	**IP地址:** 151.101.65.229 **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
mobile.events.data.microsoft.com	安全	否	**IP地址:** 13.89.178.26 **国家:** United States of America **地区:** Iowa **城市:** Des Moines **纬度:** 41.600540 **经度:** -93.609108 **查看:** Google 地图
www.telegram.me	安全	否	**IP地址:** 149.154.167.99 **国家:** United Kingdom of Great Britain and Northern Ireland **地区:** England **城市:** Warrington **纬度:** 52.184460 **经度:** -0.687590 **查看:** Google 地图
in.appcenter.ms	安全	否	**IP地址:** 40.70.161.102 **国家:** United States of America **地区:** Virginia **城市:** Boydton **纬度:** 36.667641 **经度:** -78.387497 **查看:** Google 地图
install.appcenter.ms	安全	否	**IP地址:** 13.107.213.69 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **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

api.appcenter.ms	安全	否	**IP地址:** 13.107.213.71 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
data.flurry.com	安全	否	**IP地址:** 98.136.147.18 **国家:** United States of America **地区:** New York **城市:** New York City **纬度:** 40.731323 **经度:** -73.990089 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://www.bing.com • https://raw.githubusercontent.com/Hackl0us/SS-Rule-Snippet/master/LAZY_RULES/clash.yml	自研引擎分析结果
• https://api.appcenter.ms/v0.1	com/microsoft/appcenter/distribute/Distribute.java
• 172.19.0.1 • 172.19.0.2	com/worldpass/app/vpn/service/TunService.java
• https://install.appcenter.ms • https://in.appcenter.ms • https://github.com/dreamacro/clash • https://mobile.events.data.microsoft.com/onecollector/1.0 • https://github.com/sharmajv/vpn • https://raw.githubusercontent.com/sharmajv/vpn/main/config.json • https://github.com/kr328/clashforandroid/releases • http://www.telegram.me/ • 172.19.0.1 • https://api.appcenter.ms/v0.1 • https://github.com/dreamacro/clash/wiki • https://donate.kr328.app • https://github.com/kr328/clashforandroid/issues • https://github.com/kr328/clashforandroid • https://issuetracker.google.com/issues/116541301 • https://cdn.jsdelivr.net/gh/sharmajv/vpn@main/config.json • https://data.flurry.com/v1/flr.do • 172.19.0.2 • https://a.yondo.com/mb/ossw67bhnmlvpc0	自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Clash Core	Dreamacro	A rule-based tunnel in Go.
App Center	Microsoft	Visual Studio App Center 将多个通用服务整合到 DevOps 云解决方案中。开发人员使用 App Center 来构建，测试和分发应用程序。部署应用程序后，开发人员可以使用 Analytics 和 Diagnostics 服务监视应用程序的状态和使用情况。

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

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 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。

第三方追踪器检测

名称	类别	网址
Flurry	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/25
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

敏感凭证泄露检测

可能的密钥
"authentication" : "Authentication"
"key" : "键"
"key" : "鍵"
"bypass_private_network" : "略過私有網路"
"key" : "Key"
"authentication" : "認證"
"bypass_private_network" : "繞過私有網絡"
"bypass_private_network_summary" : "略過私有網路位址"
"bypass_private_network" : "绕过私有网络"
"authentication" : "认证"
"bypass_private_network_summary" : "绕过私有网络地址"
"bypass_private_network_summary" : "繞過私有網絡地址"
21d71b07-55b8-4140-b90a-5597d32fb4a
344f4abf0a10cb27a43[illegible]1b449c9

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

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