南明离火
移动应用检测平台

ANDROID 静态分析报告

TandagPride VPN • V1.0.0

分析日期: 2024-03-11 17:46:11

应用概览

文件名称:	TandagPride VPN.apk
文件大小:	4.12MB
应用名称:	TandagPride VPN
软件包名:	com.romzkie.paidvpn
主活动:	com.romzkie.paidvpn.LauncherActivity
版本号:	1.0.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	1/432
杀软检测:	6 个杀毒软件报毒
MD5:	e179030831eba5f89d96bd9b26ae805e
SHA1:	120900cf8f9fe02b7cd77e7422d57fa274f34e88
SHA256:	f9e4da3e2fdff3a5ea591a55c2cf548e833ec4742124506615c4efaf062027460

分析结果严重性分布

高危	中危	信息	安全	关注
3	3	2	2	0

四大组件导出状态统计

Activity组件：9个，其中export的有： 1个
Service组件：3个，其中export的有： 0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

二进制文件已签名

v1 签名: True
v2 签名: False
v3 签名: False
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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587d04d89b7711292a4569

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.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	获取网络状态	允许应用程序查看所有网络的状态。
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.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.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.startForegr ound，用于podcast播放（推送悬浮播放，锁屏播放）
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。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 警告: **0** | 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	高危	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: **5** | 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。
3	Activity设置了TaskAffinity属性 (com.romzkie.ultrasshservice.LaunchVpn)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
4	Activity (com.romzkie.ultrasshservice.LaunchVpn) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，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。
5	Broadcast Receiver (com.romzkie.ultrasshservice.MainReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，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。

代码安全漏洞检测

高危: **2** | 警告: **6** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
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
4	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

5	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: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	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
8	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	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
10	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	此应用程序使用SSL Pinning来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
12	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	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/libtool-checker.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。		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。	No RPATH 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

2	arm64-v8a/pdnsd.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。		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
3	arm64-v8a/tun2socks.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。		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	0/30	
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE

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
notes.sikatpinoy.com	安全	否	**IP地址:** 50.28.59.161 **国家:** United States of America **地区:** Michigan **城市:** Lansing **纬度:** 42.733280 **经度:** -84.637704 **查看:** Google 地图
t.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:** 52.184400 **经度:** -0.687590 **查看:** Google 地图
jsocks.sourceforge.net	安全	否	**IP地址:** 172.64.150.145 **国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://notes.sikatpinoy.com/raw/0hJ2csFFgdt	com/romzkie/paidvpn/LoginActivity.java
• https://notes.sikatpinoy.com/raw/xfa2QqxMHt • http://https://notes.sikatpinoy.com/raw/xfa2QqxMHt	com/romzkie/paidvpn/activities/SMS_Updater.java
• https://notes.sikatpinoy.com/raw/uHC7CKC222	com/romzkie/paidvpn/util/ConfigUpdate.java
• 1.1.1.1	com/romzkie/ultrasshservice/config/Settings.java
• 8.8.8.8	com/romzkie/ultrasshservice/tunnel/vpn/Tunnel.java
• 8.8.8.8 • 8.8.4.4	com/romzkie/ultrasshservice/tunnel/vpn/TunnelConstants.java

• 8.8.4.4 • 8.8.8.8 • 10.0.0.1 • 10.0.0.2 • 172.16.0.1 • 172.16.0.2 • 192.168.0.1 • 192.168.0.2 • 169.254.1.1 • 169.254.1.2	com/romzkie/ultrasshservice/tunnel/vpn/VpnUtils.java
• 172.16.0.1 • 10.0.0.1 • 8.8.4.4 • 1.1.1.1 • 169.254.1.1 • 192.168.0.1 • 8.8.8.8 • https://notes.sikatpinoy.com/raw/uHC7CKCqz2 • https://github.com/jenkinsci/trilead-ssh2 • 169.254.1.2 • http://t.me/SlipkProjects • https://notes.sikatpinoy.com/raw/xfa2QqxMHt • https://jsocks.sourceforge.net • 10.0.0.2 • 192.168.0.2 • https://notes.sikatpinoy.com/raw/OHzosFFgdt • 172.16.0.2	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
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
zlib@openssh.com	com/trilead/ssh2/compression/CompressionFactory.java
zlib@openssh.com	自研引擎分析结果
p.a.rombouts@home.nl tmoestl@gmx.net	lib/arm64-v8a/pdnsd.so
ambrop7@gmail.com	lib/arm64-v8a/tun2socks.so

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

敏感凭证泄露检测

可能的密钥
"state_auth" : "Authenticating"
"state_auth_success" : "Authenticated"
"state_auth" : "Verificando"
"auth_username" : "Username"
"state_auth_success" : "Verificado"
"proxy_user" : "User"
"password" : "Password"
"password" : "Contraseña"
3617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995F42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
1797693134862315907708391567937874531978602960487 5
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208
a3785913ca4deb75abd841414d0a700098e879777940c78c73fe6f2bee6c0352
552BB9ED529077096966D670C354E4ABC9804F1746D08CA18217C32905E462E36C
AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB7
00C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66
027081084290769293204912819446762700 7
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
00742530207447712589550957937778[illegible]4442426617334727629299387668709205606 05
A6DF25F14374FE1356D6D51245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB
6F406B7EDEE386BFB3A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A
b0a00e4a271b[illegible]42fad0618432fa7d7fb3d99004d2b0bdfc14f8024832b
B3312FA7[illegible]E7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129
6011706444423684197180216158519368947833795864925541502180565485980503646 4

024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0
83995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF
405481992391000507928770033558166392295531362390765087357599148225748625 75
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
E3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF69558171
6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296

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患。