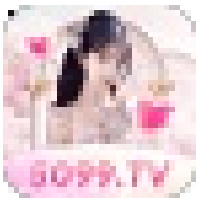
ANDROID 静态分析报告



天宫 • v5.0.2

分析日期: 2024-07-18 16:14:17

应用概览

文件名称:	tiangong-p8YYW-vc504eaaf-x64.apk
文件大小:	38.27MB
应用名称:	天宫
软件包名:	com.MNe1vopIjTK7h56v.yk3aYQhflHVrTnLW
主活动:	com.xkJRAsHIndFABaEX.HIluiPGSUUQWugXj.MainActivity
版本号:	5.0.2
最小SDK:	23
目标SDK:	33
加固信息:	资源混淆
应用程序安全分数:	58/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	1f4afaea77fa036559231c54bdec09af
SHA1:	8fce5811c5653f3286a2d06d83701fcae0d9d32e
SHA256:	ba0e97fc6d0576fbc7806e378f3b1d87e6c28863f19bb91c4c17e27e022bbf9

分析结果严重性分布

高危	中危	信息	安全	关注
0	7	0	1	0

四大组件导出状态统计

Activity组件：4个，其中export的有：0个
Service组件：2个，其中export的有：1个
Receiver组件：4个，其中export的有：3个
Provider组件：4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: False
v2 签名: True
v3 签名: False

v4 签名: False
主题: C=CN, ST=BeiJing, L=BeiJing, O=aiNewieg, OU=Ahkuichu, CN=oneehooB
签名算法: dsa
有效期自: 2024-07-18 03:31:43+00:00
有效期至: 2039-07-15 03:31:43+00:00
发行人: C=CN, ST=BeiJing, L=BeiJing, O=aiNewieg, OU=Ahkuichu, CN=oneehooB
序列号: 0x48c2b0de
哈希算法: sha256
证书MD5: d336fd08d5648e4eedac83861817b247
证书SHA1: 5fd54d30a893573551c73307172fe5a0c053418d
证书SHA256: ad58f19374c056a6014dc42b99f7558af34d8ebd33811e8faf3b2f84f60b8db8
证书SHA512:
36948c72ce9827c8866a2893b2d60fef43eb9e08fe68a752c5b5d8f01c2923b42be12f0517260208896d89c44251007afd4445687655844a0e8b74b766da57

公钥算法: dsa
密钥长度: 2048
指纹: 748919c68fae8ccc07bdae0f1acd346ce227ae5772e29d1848702bda1d32f2f6
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.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.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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
com.MNe1vopljTK7h56v.yk3aYOnfIhVrTnLW.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
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.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.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_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.startForegrond，用于podcast播放（播送是浮播放，锁屏播放）
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。

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: **0** | 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

Manifest 配置安全分析

高危: **0** | 警告: **6** | 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 6.0-6.0.1, [minSdk=23]	信息	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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	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	Broadcast Receiver (com.github.florent37.assets_audio_player.notification.bPNqsywVCKYwSaYQ) 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。
5	Broadcast Receiver (com.github.florent37.assets_audio_player.notification.FjEBVCoDYtVviNxK) 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。
6	Service (com.github.florent37.assets_audio_player.notification.bSMSFDBGPCxTTdew) 未被保护。 [android:exported=true]	警告	发现 Service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。
7	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。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

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/libtunkohmf.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk', '__read_chk', '__vsprintf_chk', '__memset_chk']	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	13/30	android.permission.WRITE_SETTINGS android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.PACKAGE_USAGE_STATS android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.CAMERA
其它常用权限	9/46	android.permission.FLASHLIGHT android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.BLUETOOTH android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_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。

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.awrcLMdDbm.tzlWIQJtjTd.key" : "true"
凭证信息=> "com.tMrCWXTzHOIRVqfp.APP_KEY" : "EYBPvLKyxGqdmDLH"

免责声明及风险提示: