南明离火
移动应用检测平台

ANDROID 静态分析报告

Tasker • v6.2.22

分析日期: 2025-04-03 00:28:40

应用概览

文件名称:	Tasker v6.2.22.apk
文件大小:	33.32MB
应用名称:	Tasker
软件包名:	net.dinglisch.android.taskerm
主活动:	net.dinglisch.android.taskerm.Tasker
版本号:	6.2.22
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	40/100 (中风险)
杀软检测:	4 个杀毒软件报毒
MD5:	38e97711a9d1bc26fce087a120abaee6
SHA1:	e6e3a4861259e058ecd704e5d34a67c8d75b8cda
SHA256:	5a03c3e2caf2a9c604ca1dd1d91e3e3206587118ee[illegible]a88119aef784a90066

分析结果严重性

高危	中危	信息	安全	关注
22	72	3	3	1

四大组件信息

Activity组件：75个，其中export的有：25个
Service组件：25个，其中export的有：18个
Receiver组件：15个，其中export的有：13个
Provider组件：4个，其中export的有：2个

证书信息

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=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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d7958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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。
net.dinglisch.android.zoom.permission.MAKE_CHANGES	未知	未知权限	来自 android 引用的未知权限。
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
cyanogenmod.permission.PUBLISH_CUSTOM_TILE	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.REQUEST_COMPANION_RUN_IN_BACKGROUND	普通	允许配套应用程序在后台运行	允许配套应用在后台运行。
android.permission.REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	普通	允许配套应用程序在后台使用数据	允许配套应用在后台使用数据。
android.permission.BODY_SENSORS	危险	授予对身体传感器的访问权限，例如心率	允许应用程序访问来自传感器的数据，用户使用这些传感器来测量身体内部发生的事情，例如心率。
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
com.latedroid.juicedefender.permission.CONTROL_JUICEDEFENDER	未知	未知权限	来自 android 引用的未知权限。
com.latedroid.juicedefender.permission.TOGGLE_MOBILE_DATA	未知	未知权限	来自 android 引用的未知权限。

android.permission.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
com.android.phone.CHANGE_NETWORK_MODE	未知	未知权限	来自 android 引用的未知权限。
android.permission.SET_TIME_ZONE	危险	设置时区	允许应用程序设置时区。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
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.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.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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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.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粗略的经纬度信息，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。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
android.permission.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
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.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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。

本报告由南明离火移动安全分析平台生成

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。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、重行转接甚至阻止外拨电话。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
android.permission.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.DUMP	签名(系统)	获得系统内部状态	允许应用程序检索系统的内部状态。恶意应用程序可借此检索它们本不需要的各种保密信息和安全信息。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
android.permission.TETHER_PRIVILEGED	未知	未知权限	来自 android 引用的未知权限。
com.joaomgcd.taskersettings.SET_SETTING	未知	未知权限	来自 android 引用的未知权限。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
android.permission.CAPTURE_AUDIO_OUTPUT	签名(系统)	允许捕获音频输出	允许应用程序捕获音频输出。
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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。

android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.SET_MEDIA_KEY_LISTENER	未知	未知权限	来自 android 引用的未知权限。
android.permission.SET_WALLPAPER_COMPONENT	签名(系统)	设置壁纸组件	允许应用程序设置壁纸组件。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.ACCESS_WIMAX_STATE	未知	未知权限	来自 android 引用的未知权限。
android.permission.CHANGE_WIMAX_STATE	未知	未知权限	来自 android 引用的未知权限。
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_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.HIGH_SAMPLING_RATE_SENSORS	普通	传感器的数据刷新率限制	允许应用以大于 200 Hz 的采样率访问传感器数据，此数据包括由设备的加速度、陀螺仪和磁力传感器记录的值。
android.permission.READ_CLIPBOARD_IN_BACKGROUND	未知	未知权限	来自 android 引用的未知权限。
android.permission.SET_VOLUME_KEY_LONG_PRESS_LISTENER	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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.SET_PROCESS_LIMIT	危险	限制运行的进程个数	允许应用程序控制将运行的进程数上限。普通应用程序从不需要使用此权限。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.wireguard.android.permission.CONTROL_TUNNELS	未知	未知权限	来自 android 引用的未知权限。
com.termux.permission.RUN_COMMAND	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。

android.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
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.CALL_COMPANION_APP	普通	使 InCallService 应用程序能够充当呼叫伴侣	允许实现InCallServiceAPI的应用 有资格作为调用配套应用启用。
android.permission.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH_PRIVILEGED	签名(系统)	允许特权蓝牙操作，无需用户交互	允许应用程序在没有用户交互的情况下配对蓝牙设备，并允许或禁止电话簿访问或消息访问。
android.permission.NEARBY_WIFI_DEVICES	危险	需要通过 Wi-Fi 进行广告和连接到附近的设备	需要能够通过 Wi-Fi 进行广告宣传和连接到附近的设备。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.BATTERY_STATS	普通	修改电池统计	允许对手机电池统计信息进行修改
android.permission.MODIFY_QUIET_MODE	未知	未知权限	来自 android 引用的未知权限。
moe.shizuku.manager.permission.API_V23	未知	未知权限	来自 android 引用的未知权限。
net.dinglisch.android.taskerm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
com.joaomgcd.taskerm.net.auth.ActivityHttpAuthentication	Schemes: tasker://, Hosts: auth,
com.joaomgcd.taskerm.util.ActivitySecondaryApp	Schemes: tasker://, Hosts: secondary,

net.dinglisch.android.taskerm.IntentHandler	Schemes: task://, http://, file://, Hosts: *, Mime Types: tasker/task, text/*, Path Patterns: .*\\.prf\\.xml, .*\\.tsk\\.xml, .*\\.scn\\.xml, .*\\.prj\\.xml,
com.joaomgcd.taskerm.datashare.import.ActivityImportTaskerDataFromUri	Schemes: taskershare://, taskertask://, taskerprofile://, taskerproject://, Hosts: *,
com.joaomgcd.taskerm.datashare.import.ActivityPreviewTaskerDataFromUri	Schemes: taskersharepreview://, Hosts: *,
com.joaomgcd.taskerm.settings.ActivityOpenSetting	Schemes: taskersetting://, Hosts: *,
com.joaomgcd.taskerm.util.ActivityAssistantActions	Schemes: tasker://, Hosts: assistantactions,

网络通信安全

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

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为信任用户安装的证书。

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **18** | 警告: **61** | 信息: **2** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Service (net.dinglisch.android.taskerm.MyVpnService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VPN_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。
5	Activity (com.joaomgcd.taskerm.net.auth.ActivityHttpAuthentication) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
6	Activity (com.joaomgcd.taskerm.net.auth.ActivityHttpAuthentication) 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。
7	Content Provider (net.dinglisch.android.taskerm.MyContentProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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 (net.dinglisch.android.taskerm.Tasker) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity (com.joaomgcd.taskerm.util.ActivitySecondaryApp) 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。
10	Activity (net.dinglisch.android.taskerm.LongPressSearch) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity (net.dinglisch.android.taskerm.LongPressSearch) 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。
12	Activity (net.dinglisch.android.taskerm.Settings) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (net.dinglisch.android.taskerm.Settings) 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。
14	Activity (net.dinglisch.android.taskerm.MIDIHandler) 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。

15	Activity (net.dinglisch.android.taskerm.WebSearchHandler) 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。
16	Activity (net.dinglisch.android.taskerm.AssistHandler) 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。
17	Service (com.joaomgcd.taskerm.assistant.ServiceVoiceInteractionTasker) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VOICE_INTERACTION [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。
18	Service (com.joaomgcd.taskerm.assistant.ServiceVoiceInteractionSessionTasker) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_VOICE_INTERACTION [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。
19	Activity (net.dinglisch.android.taskerm.IntentHandler) 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。
20	Activity (net.dinglisch.android.taskerm.TaskSelect) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
21	Activity (net.dinglisch.android.taskerm.TaskSelect) 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。
22	Activity (net.dinglisch.android.taskerm.DockActivityCar) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
23	Activity (net.dinglisch.android.taskerm.DockActivityCar) 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。
24	Activity (net.dinglisch.android.taskerm.DockActivityDesk) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。

25	Activity (net.dinglisch.android.taskerm.DockActivityDesk) 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。
26	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetConfigure) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
27	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetConfigure) 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。
28	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetConfigureShortcut) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
29	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetConfigureShortcut) 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。
30	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetCountdownConfigure) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
31	Activity (net.dinglisch.android.taskerm.TaskerAppWidgetCountdownConfigure) 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。
32	Activity (com.joaomgcd.taskerm.util.ActivityTileLongClick) 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。
33	Service (net.dinglisch.android.taskerm.QSTileService0) 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。
34	Service (net.dinglisch.android.taskerm.QSTileService1) 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。

35	Service (net.dinglisch.android.taskerm.QSTileService2) 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。
36	Service (net.dinglisch.android.taskerm.NotificationListenerService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_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。
37	Service (net.dinglisch.android.taskerm.MyAccessibilityService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_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。
38	Broadcast Receiver (net.dinglisch.android.taskerm.IpackReceiver) 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。
39	Activity (net.dinglisch.android.taskerm.IpackIconSelect) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
40	Activity (net.dinglisch.android.taskerm.IpackIconSelect) 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。
41	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticPhoneState) 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。
42	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticCallRewriter) 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。
43	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticCallBlocker) 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。

44	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticAlwaysOn) 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。
45	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticRunTasks) 受权限保护，但是应该检查权限的保护级别。 Permission: net.dinglisch.android.tasker.PERMISSION_RUN_TASKS protectionLevel: dangerous [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。它受到一个权限的保护。然而，这个权限的保护级别被设置为危险。这意味着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。
46	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticInternal) 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。
47	Broadcast Receiver (net.dinglisch.android.taskerm.ReceiverStaticExternal) 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。
48	Broadcast Receiver (net.dinglisch.android.taskerm.TaskerAppWidgetProvider) 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。
49	Broadcast Receiver (net.dinglisch.android.taskerm.TaskerAppWidgetCountdownProvider) 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。
50	Broadcast Receiver (net.dinglisch.android.taskerm.MyDeviceAdminReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [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。
51	Service (com.joaomgcd.taskerm.plugin.ServiceRequestQuery) 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。
52	Service (com.joaomgcd.taskerm.plugin.ServicePluginFinished) 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。

53	Activity (com.joaomgcd.taskerm.datashare.import.ActivityImportTaskerDataFromXml) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
54	Activity (com.joaomgcd.taskerm.datashare.import.ActivityImportTaskerDataFromXml) 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。
55	Activity (com.joaomgcd.taskerm.datashare.import.ActivityImportTaskerDataFromUri) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
56	Activity (com.joaomgcd.taskerm.datashare.import.ActivityImportTaskerDataFromUri) 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。
57	Activity (com.joaomgcd.taskerm.datashare.import.ActivityPreviewTaskerDataFromUri) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
58	Activity (com.joaomgcd.taskerm.datashare.import.ActivityPreviewTaskerDataFromUri) 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。
59	Service (com.joaomgcd.taskerm.keyboard.InputMethodServiceTasker) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_INPUT_METHOD [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。
60	Activity (com.joaomgcd.taskerm.nfc.ActivityNFCTag) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
61	Activity (com.joaomgcd.taskerm.nfc.ActivityNFCTag) 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。
62	Activity (com.joaomgcd.taskerm.navigationbar.ActivityReceiveKey) 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。

63	Content Provider (com.joaomgcd.taskerm.navigationbar.IconProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
64	Broadcast Receiver (com.joaomgcd.taskerm.event.datetime.BroadcastReceiverNextAlarmChanged) 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。
65	Activity (com.joaomgcd.taskerm.settings.ActivityOpenSetting) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
66	Activity (com.joaomgcd.taskerm.settings.ActivityOpenSetting) 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。
67	Service (com.joaomgcd.taskerm.controlsprovider.ControlsProviderServiceTasker) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_CONTROLS [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。
68	Service (com.joaomgcd.taskerm.command.ServiceSendCommand) 受权限保护，但是应该检查权限的保护级别。 Permission: net.dinglisch.android.tasker.PERMISSION_SEND_COMMAND protectionLevel: dangerous [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。它受到一个权限的保护。然而，这个权限的保护级别被设置为危险。这意味着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。
69	Activity (com.joaomgcd.taskerm.util.ActivityAssistantActions) 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。
70	Service (com.joaomgcd.taskerm.call.ServiceCallScreening) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_SCREENING_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。
71	Service (com.joaomgcd.taskerm.call.ServiceCallCompanion) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_INCALL_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。

72	Activity (com.joaomgcd.oldtaskercompat.matter.ActivityMatterHandleCommissionDeviceRequest) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
73	Activity (com.joaomgcd.oldtaskercompat.matter.ActivityMatterHandleCommissionDeviceRequest) 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。
74	Service (com.joaomgcd.oldtaskercompat.matter.ServiceMatterCommissioning) 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。
75	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。
76	Activity (androidx.core.google.shortcuts.TrampolineActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
77	Activity (androidx.core.google.shortcuts.TrampolineActivity) 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。
78	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。
79	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。
80	高优先级的Intent (999) - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

高危: **2** | 警告: **9** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
3	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
4	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
5	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
6	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
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	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

9	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
10	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
11	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
12	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
13	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
14	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
15	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
16	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

动态库分析

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/libCHIPController.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。	动态共享对象 (DSO) 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技术。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	True info 二进制文件有以下加固函数: ['__FD_ISSET_chk', '__FD_SET_chk']	True info 符号被剥离

2	arm64-v8a/libSetupPayloadParser.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。	动态共享对象 (DSO) 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技术。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

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
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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	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
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限

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
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00100	检查网络连通性	信息收集 网络	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00127	监视广播操作事件（BOOT_COMPLETED等）	命令	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00136	停止录音	录制音视频 命令	升级会员：解锁高级权限
00092	发送广播	命令	升级会员：解锁高级权限
00133	开始录音	录制音视频 命令	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限

00210	将最新渲染图像中的像素复制到位图中	信息收集	升级会员：解锁高级权限
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00058	连接到特定的WIFI网络	WiFi 控制	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
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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	升级会员：解锁高级权限
00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
00060	查询网络运营商名称	网络 信息收集	升级会员：解锁高级权限
00061	返回有关当前 Wi-Fi 连接的动态信息	WiFi 信息收集	升级会员：解锁高级权限
00038	查询电话号码	信息收集	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
00130	获取当前WIFI信息	WiFi 信息收集	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
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
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	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
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
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	短信 通话记录 信息收集	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限

00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	27/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.PACKAGE_USAGE_STATS android.permission.WRITE_CALL_LOG android.permission.READ_CALL_LOG android.permission.RECEIVE_SMS android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.WRITE_SETTINGS android.permission.RECORD_AUDIO android.permission.READ_PHONE_STATE android.permission.SEND_SMS android.permission.WRITE_SMS android.permission.READ_SMS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.SET_WALLPAPER android.permission.MODIFY_AUDIO_SETTINGS android.permission.PROCESS_OUTGOING_CALLS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.CALL_PHONE android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.SYSTEM_ALERT_WINDOW

其它常用权限	18/46	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.ACTIVITY_RECOGNITION android.permission.ACCESS_BACKGROUND_LOCATION android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_IMAGES android.permission.BATTERY_STATS

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。

域名检测

域名	状态	中国境内	位置信息
www.xda-developers.com	安全	否	**IP地址:** 52.5.96.96 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
goo.gle	安全	否	**IP地址:** 67.199.248.12 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图
zoom.dinglisch.net	安全	否	No Geolocation information available.
securesettings.intangibleobject.com	安全	否	**IP地址:** 142.250.68.83 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.patreon.com	安全	否	**IP地址:** 104.16.24.14 **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

www.tacit.dk	安全	否	**IP地址:** 104.21.91.201 **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
www.bing.com	安全	否	**IP地址:** 23.43.51.146 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 埃尔塞贡多 **纬度:** 33.919201 **经度:** -118.416580 **查看:** Google 地图
steelgirderdev.com	安全	否	**IP地址:** 143.95.226.49 **国家:** 美国 **地区:** 佛罗里达州 **城市:** 杰克逊维尔 **纬度:** 30.191099 **经度:** -81.493103 **查看:** Google 地图
taskernet.com	安全	否	**IP地址:** 216.239.38.21 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
tools.ietf.org	安全	否	**IP地址:** 104.16.45.99 **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
tasker.joaoapps.com	安全	否	**IP地址:** 35.192.182.63 **国家:** 美国 **地区:** 爱荷华州 **城市:** 康瑟尔布拉夫斯 **纬度:** 41.261940 **经度:** -95.860832 **查看:** Google 地图
www.regular-expressions.info	安全	否	**IP地址:** 216.92.20.37 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 匹兹堡 **纬度:** 40.424881 **经度:** -79.980957 **查看:** Google 地图
test.com	安全	否	**IP地址:** 34.224.149.186 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

www.joda.org	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
joaoapps.com	安全	否	**IP地址:** 104.155.6.62 **国家:** 比利时 **地区:** 布鲁塞尔首都大区市镇 **城市:** 布鲁塞尔 **纬度:** 50.850849 **经度:** 4.348780 **查看:** Google 地图
wiki.xiph.org	安全	否	**IP地址:** 140.211.166.31 **国家:** 美国 **地区:** 俄勒冈 **城市:** 尤金 **纬度:** 44.036083 **经度:** -123.052429 **查看:** Google 地图
buildwithmatter.com	安全	否	**IP地址:** 104.21.16.1 **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
ipack.dinglisch.net	安全	否	No Geolocation information available.
wiki.devmil.de	安全	否	No Geolocation information available.
forum.joaoapps.com	安全	否	**IP地址:** 104.196.140.79 **国家:** 美国 **地区:** 南卡罗来纳州 **城市:** 蒙克斯角 **纬度:** 33.195999 **经度:** -80.013138 **查看:** Google 地图
www.afterhoursdevelopers.com	安全	否	No Geolocation information available.
youtu.be	安全	否	**IP地址:** 172.217.12.142 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图
speex.org	安全	否	**IP地址:** 140.211.166.31 **国家:** 美国 **地区:** 俄勒冈 **城市:** 尤金 **纬度:** 44.036083 **经度:** -123.052429 **查看:** Google 地图

bla.com	安全	否	**IP地址:** 38.127.92.75 **国家:** 美国 **地区:** 华盛顿 **城市:** 塔奇拉 **纬度:** 47.442909 **经度:** -122.270233 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• http://myserver.com • http://forum.joaoapps.com/index.php?resources/ • http://tasker.joaoapps.com • https://tasker.joaoapps.com/privacy.html • http://tasker.joaoapps.com/tour.html • http://tasker.dinglisch.net/tour.html • https://github.com/dlew/joda-time-android • https://facebook.com/poedelPCS/ • http://tasker.joaoapps.com/faq-ov.html • https://taskernet.com/?public • http://m.rckmn.nl/ • http://tasker.joaoapps.com/forum • http://tasker.joaoapps.com/guides.html • http://tasker.wikidot.com • http://www.softwaremonkey.org/Code/MathEval • https://taskernet.com/?shares • http://tasker.joaoapps.com/faq.html	自研引擎-A
• https://www.xda-developers.com/android-q-google-pixel-2-pixel-3-remap-active-edge/	h9/i.java
• https://tasker.joaoapps.com/userguide/en/target_api.html	wd/g.java
• http://zoom.dinglisch.net/zoom.apk • https://play.google.com/store/apps/details?id=com.codecarpet.apndroid.pro	net/dinglisch/android/taskerm/Kid.java
• 127.0.0.1	s5/c0.java
• http://tasker.joaoapps.com/download.html	net/dinglisch/android/taskerm/TaskerIntent.java
• https://www.regular-expressions.info/tutorial.html	com/joaomgcd/taskerm/pattern/RegexHelper.java
• https://tasker.joaoapps.com/userguide/en/matching.html	na/b.java
• https://cloud.google.com/text-to-speech/docs/ssml	com/joaomgcd/taskerm/action/alert/l.java
• https://tasker.joaoapps.com/userguide/en/target_api.html	com/joaomgcd/taskerm/action/net/b1.java
• http://test.com?	v9/q.java
• https://accounts.google.com/o/oauth2/v2/auth	w9/e.java

• https://youtu.be/uy4owfsbqks • https://tasker.joaoapps.com/profiles • https://tasker.joaoapps.com/privacy.html • https://youtu.be/bcj3a-pzf5k • https://youtu.be/rkqrh17h-dy • https://youtu.be/oufvnh_9rd0 • https://tasker.joaoapps.com/changes.html • https://youtu.be/gga4ofxmlzu • https://tasker.joaoapps.com/guides.html • https://drive.google.com/file/d/1vv9eifneslw99brlckz-qecsrok6k_81/view • https://youtu.be/ja8sv7uissg?tasker=true • https://tasker.joaoapps.com/userguide/en/faqs/faq-problem.html#00 • https://youtu.be/s6eablw5wsk	net/dinglisch/android/taskerm/Main.java
• https://tasker.joaoapps.com/auth.html	w9/d.java
• https://youtu.be/zxxfowle29i	com/joaomgcd/taskerm/datashare/export/ShareDataConfig.java
• https://accounts.google.com/o/oauth2/revoke?token=	x4/d.java
• https://drive.google.com/file/d/	com/joaomgcd/taskerm/google/drive/io/DriveMetadata.java
• https://youtu.be/t3cbs3aez6m	com/joaomgcd/taskerm/nfc/ActivityNFCTag.java
• https://play.google.com/store/apps/details?id=com.icecoldapps.screenshoteasy • https://play.google.com/store/apps/details?id=com.terdelle.twilight • https://play.google.com/store/apps/details?id=com.joaomgcd.automotification • http://www.afterhoursdevelopers.com/applications/android/syncer-android-sync-widget • https://play.google.com/store/apps/details?id=com.benfinnigan.wol • https://play.google.com/store/apps/details?id=com.joaomgcd.autoremote • http://securesettings.intangibleobject.com/ • http://wiki.devmil.de/tiki-index.php • http://www.tacit.dk/foldersync • https://play.google.com/store/apps/details?id=com.icecoldapps.serversultimate • https://play.google.com/store/apps/details?id=org.kman.aquamail • https://play.google.com/store/apps/details?id=com.icecoldapps.synchronizeultimate • https://play.google.com/store/apps/details?id=com.joaomgcd.autoshare • https://play.google.com/store/apps/details?id=com.joaomgcd.autoshortcut • https://play.google.com/store/apps/details?id=com.joaomgcd.autoinput • http://steelgirderdev.com/steelgirderdev/gvsettings.html • https://play.google.com/store/apps/details?id=com.chasarin.android.udpsender • https://play.google.com/store/apps/details?id=com.joaomgcd.autocast • https://play.google.com/store/apps/details?id=com.balda.touchtask • https://play.google.com/store/apps/details?id=com.devuni.flashlight.tasklight • https://play.google.com/store/apps/details?id=pt.joaormf.mtkcontrol • https://play.google.com/store/apps/details?id=net.nurik.roman.dashclock • https://play.google.com/store/apps/details?id=se.badaccess.locale.nfc • https://play.google.com/store/apps/details?id=com.asif.plugin.sendexpect	net/dinglisch/android/taskerm/wg.java
• https://tasker.joaoapps.com/userguide/en/variables.html#json	com/joaomgcd/taskerm/dialog/a.java
• https://tools.ietf.org/html/rfc5574 • https://wiki.xiph.org/oggopus • https://speex.org/	com/joaomgcd/taskerm/google/speechtotext/RequestRecognize$RecognitionConfig.java
• https://tasker.joaoapps.com/userguide/en/help/ah_secure_setting_grant.html	com/joaomgcd/taskerm/assistant/ServiceVoiceInteractionTasker.java

• https://taskernet.com/shares/	net/dinglisch/android/taskerm/wl.java
• https://tasker.joaoapps.com/userguide/en/faqs/faq-problem.html#00	com/joaomgcd/tasky/taskyroutine/intro/ViewModelTaskyIntro.java
• https://taskernet.com/?public • https://forum.joaoapps.com/index.php?resources	com/joaomgcd/taskerm/helper/p.java
• https://tasker.joaoapps.com/userguide/en/help/ah_adb_wifi.html	c8/e.java
• https://www.joda.org/joda-time/apidocs/org/joda/time/format/datetimeformat.html	b8/e0.java
• https://www.regular-expressions.info/tutorial.html	b8/f0.java
• https://tasker.joaoapps.com/userguide/en/variables.html#json	b8/g0.java
• http://zoom.dinglisch.net/zoom.apk • http://zoom.dinglisch.net/	net/dinglisch/android/taskerm/en.java
• https://goo.gle/compose-feedback	f0/n.java
• https://tasker.joaoapps.com/userguide/en/variables.html#html • https://tasker.joaoapps.com/userguide/en/variables.html#json	net/dinglisch/android/taskerm/mn.java
• https://tasker.joaoapps.com/userguide/en/variables.html#json	h9/e.java
• https://play.google.com/store/apps/details?id= • https://play.google.com/apps/testing/ • https://tasker.joaoapps.com/userguide/ • https://www.patreon.com/joaoapps • https://joaoapps.com	com/joaomgcd/taskerm/util/ExtensionsContextKt.java
• https://tasker.joaoapps.com/commandsystem.html	h9/d.java
• https://buildwithmatter.com/	chip/platform/PreferencesConfigurationManager.java
• https://tasker.joaoapps.com/userguide • https://tasker.joaoapps.com/userguide/	net/dinglisch/android/taskerm/HTMLView.java
• javascript:document.body.style.setproperty	db/j.java
• https://tasker.joaoapps.com/userguide/en/matching.html	net/dinglisch/android/taskerm/ActionEdit.java
• http://ipack.dinglisch.net/download.html	net/dinglisch/android/taskerm/y4.java
• 192.168.0.1 • 8.8.8.8	net/dinglisch/android/taskerm/MyVpnService.java
• https://play.google.com/store/apps/details?id= • https://bla.com • data:audio/mp3;base64	com/joaomgcd/taskerm/util/z1.java
• https://tasker.joaoapps.com/userguide/en/matching.html	com/joaomgcd/taskerm/action/input/x1.java

• http://www.bing.com/bingbot.htm • http://www.google.com/bot.html	com/joaomgcd/taskerm/action/net/i.java
• https://tasker.joaoapps.com/adbwifi • https://www.patreon.com/joaoapps • https://tasker.joaoapps.com/plugin_timeout • http://tasker.joaoapps.com/faq-problem.html#app	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 应用中运行原生代码。
Google Sign-In	Google	提供使用 Google 登录的 API。
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。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

邮箱

EMAIL	源码文件
tasker@dinglisch.net	net/dinglisch/android/taskerm/ExecuteService.java
support@joaoapps.com	com/joaomgcd/taskerm/util/w6.java
fred.smith@a.domain.com	自研引擎-S

密钥凭证

可能的密钥
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "AIzaSyDjkrU296YbCFBkDUq3KsJOG-yPS3pDNbk"
凭证信息=> "com.google.android.backup.api_key" : "AEdPqrEAAAAIloUzVq7-xvaHCcUYiu9aC2inqGijn-iW_px6eQ"
凭证信息=> "io.fabric.ApiKey" : "629283e2b45fb5d335a25270441ca429f8649fb5"
"scene_event_type_key" : "Key"
"http_auth_response_headers" : "Headers"

"word_keys" : "Tasten"
"an_keyboard" : "Clavier"
"an_keyboard" : "Teclado"
"an_keyguard_enabled" : "Keyguard"
"word_keys" : "Tasti"
"http_auth_response_headers" : "Cabeceras"
"an_keyboard" : "Keyboard"
"word_keys" : "Key"
"an_keyguard_pattern" : "Tastensperre-Muster"
"an_show_soft_keyboard" : "Tastiera"
"pl_key" : "anahtar"
"usb_class_hid_keyboard" : "HID/klavye"
"scene_event_type_key" : "Taste"
"scene_event_type_key" : "Tasto"
"word_keys" : "Keys"
"scene_event_type_key" : "Tecla"
"pl_key" : "Tasto"
"pl_key" : "Chave"
"pl_key" : "Clave"
"an_keyguard_enabled" : "Tastensperre"
"an_keyguard_enabled" : "Verrouillage"
"pl_cert_password" : "Zertifikatspasswort"
"pl_password" : "Password"
"pl_key" : "Key"
"scene_event_type_key" : "Touche"
"word_keys" : "Touches"
"an_keyboard" : "Klavye"
"scene_event_type_key" : "Anahtar"
"word_keys" : "Anahtarlar"
"pl_user_name" : "Username"
"an_show_soft_keyboard" : "Bildschirmtastatur"

"word_keys" : "Teclas"
GRsdmyyd9enbLYC3yiAf6FbWCpLyasV7YLWV97O2pAxA
ZcIgVt3pzkA7KiXdK3cdyU1Co7h2YdOlDQpBZ8DCiSpF5E5Np
eyJhdWQiOiJOWk5GUUZEUyIsImV4cCI6MjM3ODYyMzkwNywiaWF0Ijo0MzI2MDMzNjkwLCJpc3MiOiIiLCJqdGkiOiIiLCJuYmYiOjAsInN1YiI6IjkyOTAxMTQ3MjUiLCJ0eXBlIjoiIn0=
AS35m8ne7oO4s+aDx/wlzjdFTfVMWstg1ay5AkpiNdrLoSXEZdFfw1IpXiyJCVLNW0yn
n8lmvRKo7pHXY85wunns71Hvz2etzcRrR40uWLyi28UU6gHvk7gTSif5B2qy
nQCPoqFNI727nzEynGCvyU13A1xtuPbUiBLcyKA==
Vi1Y9NzcV7qTVPVruQ91ro298mQ1T6UYEcZoT8FcpAiX64ul9PQ1s4dEQJ5O

GooglePlay应用信息

标题: Tasker

评分: 4.3629937 **安装:** 1,000,000+ **价格:** 3.234241 **Android版本支持:** **分类:** 工具 **Play Store URL:** net.dinglisch.android.tasker

开发者信息: joaomgcd, 8102570190170276456, Rua Elias Garcia n17 4A 2700-310 Amadora Portugal, https://tasker.joaoapps.com/dl, support@joaoapps.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

没有重复的任务，让您的 Android 设备来处理！ 完全自动化，从设置到短信。 不仅是您可以使用 Tasker 执行的一些操作。它的真正强大之处在于可以根据您的意愿灵活地组合上下文和任务：https://tasker.joaoapps.com/examples.html 自动化 让您的手机成为真正的智能手机！当您的手机可以为您做到这一点时，为什么还要记得每天出门时调节音量呢？ 根据您所在的应用、一天中的时间、您的位置、您的Wi-Fi 网络自动执行操作b>、收到的短信或电话、当前播放的歌曲以及许多其他 (130 多个) 状态和事件！ 查看创建自动化有多么容易：https://www.youtube.com/watch?v=s6EAbLW5WSk 行动 350 多个操作可让您以前所未有的方式真正自定义您的手机！发送短信、创建通知、更改几乎任何系统设置（如 Wifi Tether、飞行模式、始终显示）、更改任何音量、控制请勿打扰、打开应用程序、文件操作、控制音乐播放、获取您的位置...您将获得主意。如果您能想到，Tasker 或许可以为您做到！ 注意：大多数功能不需要（我重复一遍不需要）root。但是，一些操作（例如某些设备上的"终止应用程序"和"移动数据"操作）需要 root。这是因为开发人员无法解决 Android 安全策略。 自动文件备份 如果您进行了这样的设置，Tasker 可以自动将您的文件备份到设备、SD 卡、USB 闪存盘甚至 Google Drive 上的特定文件夹！如果您希望即使丢失手机也能保证文件安全，这非常有用。 直接下载并安装APK 根据您的请求（如果您设置了任务），Tasker 可以自动检查网站是否有更新的 APK，从所述网站接收这些 APK 并启动任何文件的安装！ 其他触发因素 通过启动器快捷方式、快速设置图块、小部件、长按音量按钮、媒体按钮（如 BT 耳机或耳机上的按钮）、Bixby 按钮、导航栏、通知等手动触发您的操作！ 加入 - 远程任务者 添加 Join (https://play.google.com/store/apps/details?id=com.joaomgcd.join) 甚至可以让您从另一台 Android 设备或 PC 触发任务！ 场景 设计您自己的 UI 并用它来显示您想要的任何信息或触发任何任务！ 应用程序创建 创建您自己的独立应用程序以与 Tasker 应用程序工厂共享或销售：https://play.google.com/store/apps/details?id=net.dinglisch.android.appfactory 开发者友好 许多第 3 方开发人员已经允许您在他们的应用程序中执行操作并通过 Tasker 监听他们的事件/状态！ 查看其中一些：https://tasker.joaoapps.com/pluginlist.html 您还可以使用强大的 HTTP 身份验证和 HTTP 请求操作从 Tasker 调用大多数 Web API！查看 HTTP 身份验证和请求的示例视频：https://youtu.be/yAt2D1XmgUI。 7 天试用 - 一次性付款即可解锁 在这里获取：https://tasker.joaoapps.com/download.html 有用的链接 隐私政策：https://tasker.joaoapps.com/privacy.html 入门指南：https://tasker.joaoapps.com/guides.html 预制项目：https://forum.joaoapps.com/index.php?resources/ 官方支持论坛：https://groups.google.com/forum/#!forum/tasker Tasker 社区：https://www.reddit.com/r/tasker/ 无法修复通过 Play 商店评论报告的问题，因此请使用应用程序 > 菜单中的"向开发者报告问题"选项来执行此操作。 注释 1：Tasker 使用 BIND_DEVICE_ADMIN 权限来提供系统锁定功能 注释 2：Tasker 使用辅助服务来实现其某些功能，例如关闭通知托盘、检查当前打开的应用程序等。

免责声明及风险提示: