南明离火
移动应用检测平台

ANDROID 静态分析报告

xv助手 • v6.5.4

分析日期: 2025-04-08 13:58:06

应用概览

文件名称:	xv助手 v1.0.0.apk
文件大小:	18.04MB
应用名称:	xv助手
软件包名:	com.xv.script
主活动:	com.stardust.auojs.inrt.SplashActivity
版本号:	6.5.4
最小SDK:	21
目标SDK:	26
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	2d96bbac6e5f352c2dc7dc96f5f5eec0
SHA1:	9ce37884da8187b8bd76d884933[illegible]a3970206cb8
SHA256:	e2d99f760ace390132e0b[illegible]4affe4ab189b83e33[illegible]dc4d912e55056f1db7

分析结果严重性

高危	中危	信息	安全	关注
4	14	2	2	1

四大组件信息

Activity组件：10个，其中export的有：0个
Service组件：11个，其中export的有：0个
Receiver组件：2个，其中export的有：0个
Provider组件：3个，其中export的有：0个

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=CN
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-28 02:08:15+00:00
有效期至: 2049-12-16 02:08:15+00:00
发行人: C=CN
序列号: 0x204adc72
哈希算法: sha1
证书MD5: e1f04bf5e3a7acbe5afe96df91d50d3a
证书SHA1: 1af5775bd9ceb78667294299eee4e1f3e2d29226
证书SHA256: 9d0f8b7cd80ebd744973152d2aecb70e19b1d9830d4d833c872dfa0e39b835ca
证书SHA512:
38447d1b0d678231ff6dd98c9d08cf9fc74ece6c322750f42ca869e53895a414b63df924afa5392820c77f5e3a2e225b9bd29739[illegible]a9dbedad3cc3f2d17922ed

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.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.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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
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。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
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.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.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.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.ACCEPT_HANDOVER	危险	使呼叫应用程序能够继续在另一个应用程序中启动的呼叫	允许呼叫应用程序继续在另一个应用程序中发起的呼叫。 例如，一个视频通话应用程序希望在用户的移动网络上继续语音通话。

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.ACCESS_BLOBS_ACROSS_USERS	普通	允许跨用户访问数据 blob	允许应用程序跨用户访问数据 Blob。
android.permission.ACCESS_CHECKIN_PROPERTIES	签名(系统)	访问check-in的属性	允许对检入服务上传的属性进行读/写访问。普通应用程序不能使用此权限。
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。
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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.ACCESS_MEDIA_LOCATION	危险	获取照片的地址信息	更换头像，聊天图片等图片的地址信息被获取。
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.ACCOUNT_MANAGER	签名	作为帐户身份验证程序	允许应用程序访问帐户验证器（ams）。
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。
com.android.voicemail.permission.ADD_VOICEMAIL	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.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.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
android.permission.BIND_APPWIDGET	签名(系统)	选择窗口小部件	允许应用程序告诉系统哪个应用程序可以使用哪些窗口小部件。具有该权限的应用程序可以允许其他应用程序访问个人数据。普通应用程序不能使用此权限
android.permission.BIND_AUTOFILL_SERVICE	签名	AutofillServices 需要用于系统绑定	必须是自动填充服务所必需的，以确保只有系统才能绑定到它。
android.permission.BIND_CALL_REDIRECTION_SERVICE	签名	CallRedirectionServices 需要进行系统绑定	必须是CallRedirectionService, 以确保只有系统可以绑定到它。
android.permission.BIND_CARRIER_MESSAGING_CLIENT_SERVICE	签名	CarrierMessagingClientServices 需要系统保护	CarrierMessagingClientService必须使用此权限保护的子类。。
android.permission.BIND_CARRIER_MESSAGING_SERVICE	签名	绑定运营商消息服务的系统级权限	允许绑定到运营商应用程序中的服务的系统进程将具有此权限。

本报告由南明离火移动安全分析平台生成

android.permission.BIND_CARRIER_SERVICES	签名	绑定运营商服务的系统级权限	允许绑定到运营商应用中的服务的系统进程将拥有此权限。
android.permission.BIND_CHOOSER_TARGET_SERVICE	签名	ChooserTargetServices 需要进行系统绑定	必须由被要求ChooserTargetService，以确保只有系统可以绑定到它，此权限在 API 级别 30 中已弃用。
android.permission.BIND_COMPANION_DEVICE_SERVICE	普通	CompanionDeviceServices 需要用于系统绑定	Android 12 引入的一种特殊权限，它允许配套设备应用在用户同意的情况下，请求一组与配套设备类型相关的权限。
android.permission.BIND_CONDITION_PROVIDER_SERVICE	签名	required by ConditionProviderServices for system binding.	必须是ConditionProviderService, 以确保只有系统可以绑定到它
android.permission.BIND_CONTROLS	签名(系统)	允许系统UI请求第三方控件。	允许系统UI请求第三方控件以应系统要求，并由控制提供程序服务声明要求。
android.permission.BIND_DEVICE_ADMIN	签名	绑定设备管理	允许持有对象将意向发送到设备管理器。普通的应用程序一律无需此权限。
android.permission.BIND_DREAM_SERVICE	签名	DreamServices 需要进行系统绑定	必须是DreamService, 以确保只有系统可以绑定到它。
android.permission.BIND_INCALL_SERVICE	签名	InCallServices 需要进行系统绑定	必须是InCallService, 以确保只有系统可以绑定到。
android.permission.BIND_INPUT_METHOD	签名	绑定到输入法	允许手机用户绑定至输入法的顶级界面。普通应用程序从不需要使用此权限。
android.permission.BIND_MIDI_DEVICE_SERVICE	签名	MidiDeviceServices 需要进行系统绑定	必须是MidiDeviceService, 以确保只有系统可以绑定到它。
android.permission.BIND_NFC_SERVICE	签名	系统绑定到 NFC 服务所需的	必须由HostApduService 或要求OffHostApduService以确保只有系统可以绑定到它。
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerServices 需要用于系统绑定	必须是NotificationListenerService, 以确保只有系统可以绑定到。
android.permission.BIND_PRINT_SERVICE	签名	PrintServices 需要进行系统绑定	必须是PrintService, 以确保只有系统可以绑定到。
android.permission.BIND_QUICK_ACCESS_WALLET_SERVICE	签名	required by QuickAccessWalletServices for system binding.	必须由快速访问钱包服务要求，以确保只有系统才能绑定到它。
android.permission.BIND_QUICK_SETTINGS_TILE	签名(系统)	允许绑定到第三方快速设置图块	允许应用程序绑定到第三方快速设置磁贴。
android.permission.BIND_REMOTEVIEWS	签名	RemoteViewsServices 需要进行系统绑定	必须通过RemoteViewsService服务来请求，只有系统才能用。
android.permission.BIND_SCREENING_SERVICE	签名	CallScreeningServices 需要进行系统绑定	必须是CallScreeningService, 以确保只有系统可以绑定到它。

本报告由南明离火移动安全分析平台生成

android.permission.BIND_TELECOM_CONNECTION_SERVICE	签名	ConnectionServices 需要进行系统绑定	必须是ConnectionService, 以确保只有系统可以绑定到它。
android.permission.BIND_TEXT_SERVICE	签名	TextServices（例如 SpellCheckerService）需要用于系统绑定	必须由 TextService（例如 SpellCheckerService）要求以确保只有系统可以绑定到它。
android.permission.BIND_TV_INPUT	签名	TvInputServices 需要进行系统绑定	必须由电视输入服务要求，以确保只有系统才能绑定到它。
android.permission.BIND_VISUAL_VOICEMAIL_SERVICE	签名	VisualVoicemailServices 需要进行系统绑定	必须由链接要求VisualVoicemailService以确保只有系统可以绑定到它。
android.permission.BIND_VOICE_INTERACTION	签名	VoiceInteractionServices 需要进行系统绑定	必须是VoiceInteractionService, 以确保只有系统可以绑定到它。
android.permission.BIND_VPN_SERVICE	签名	VpnServices 需要进行系统绑定	必须是VpnService, 以确保只有系统可以绑定到它。
android.permission.BIND_VR_LISTENER_SERVICE	签名	VrListenerServices 需要进行系统绑定	必须是VrListenerService, 以确保只有系统可以绑定到它。
android.permission.BIND_WALLPAPER	签名(系统)	绑定到壁纸	允许手机用户绑定到壁纸的顶级界面。应该从不需要将此权限授予普通应用程序。
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_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
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.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.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.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.BROADCAST_PACKAGE_REMOVED	签名	发送应用删除的广播	允许应用程序广播一个应用程序包已经移除的通知。恶意程序可能借此终止其他应用程序的运行。
android.permission.BROADCAST_SMS	签名	发送已收到短信的广播	允许应用程序广播已收到短信的通知。恶意应用程序可借此伪造收到的短信。
android.permission.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。

本报告由南明离火移动安全分析平台生成

android.permission.BROADCAST_WAP_PUSH	签名	发送WAP-PUSH接收的广播	允许应用程序广播通知：WAP-PUSH消息已收到。恶意的应用程序可以使用这个伪造MMS消息的接收凭证或悄悄利用恶意变种替换任何网页的内容。
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.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.CALL_PRIVILEGED	签名(系统)	直接拨打任何电话号码	允许应用程序在您不介入的情况下拨打任何电话（包括紧急呼救）。恶意应用程序可借此向应急服务机构拨打骚扰电话甚至非法电话。
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.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.CHANGE_COMPONENT_ENABLED_STATE	签名(系统)	启用或禁用应用程序组件	允许应用程序更改是否启用其他应用程序的组件。恶意应用程序可借此停用重要的手机功能。使用此权限时务必谨慎，因为这可能导致应用程序组件进入不可用、不一致或不稳定的状态
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.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.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.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.CLEAR_APP_CACHE	危险	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件释放手机存储空间。通常此权限只适用于系统进程。
android.permission.CONTROL_LOCATION_UPDATES	签名(系统)	控制定位更新	允许获得移动网络定位信息改变。普通应用程序不能使用此权限。
android.permission.DELETE_CACHE_FILES	签名(系统)	删除缓存文件	允许应用删除缓存文件。
android.permission.DELETE_PACKAGES	签名(系统)	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可借此删除重要的应用程序。
android.permission.DIAGNOSTIC	签名	读取/写入诊断所拥有的资源	允许应用程序读取/写入诊断组所拥有的任何资源（例如，/dev 中的文件）。这可能会影响系统稳定性和安全性。此权限仅供制造商或运营商诊断硬件问题。
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.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.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.FACTORY_TEST	签名	在出厂测试模式下运行	作为一项低级制造商测试来运行，从而允许对手机硬件进行完全访问。此权限仅当手机在制造商测试模式下运行时才可用。

android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.GET_ACCOUNTS_PRIVILEGED	签名(系统)	授予对帐户服务的访问权限	允许访问帐户服务中的帐户列表。
android.permission.GET_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
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.GLOBAL_SEARCH	签名(系统)	全局搜索	此权限可以在内容提供商用来允许全球搜索系统来访问他们的数据。
android.permission.HIDE_OVERLAY_WINDOWS	普通	隐藏应用叠加窗口	允许应用防止在其上绘制非系统覆盖窗口。
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计、陀螺仪和磁力传感器记录的值。
android.permission.INSTALL_LOCATION_PROVIDER	签名(系统)	安装位置提供商	创建用于测试的模拟位置信息源。恶意程序可以用它来覆盖由真实位置信息源，如GPS或网络提供商返回的位置或状态，或者监视和报告您的位置到外部源。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
android.permission.INSTANT_APP_FOREGROUND_SERVICE	签名(系统)	允许即时应用程序创建前台服务	允许即时应用程序创建前台服务。
android.permission.INTERACT_ACROSS_PROFILES	普通	enables interaction across profiles in the same group.	允许在同一配置文件组中的配置文件之间进行交互。
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.LAUNCH_MULTI_PANE_SETTINGS_DEEP_LINK	普通	允许显示嵌入在"设置"应用程序中的活动	应用程序需要此权限 Settings.ACTION_SETTINGS_EMBED_DEEP_LINK_ACTIVITY才能显示其 Activity嵌入在设置应用程序中。
android.permission.LOADER_USAGE_STATS	签名(系统)	allows data loaders to read package access logs.	允许数据加载器读取包的访问日志。
android.permission.LOCATION_HARDWARE	普通	允许使用硬件中的定位功能	允许应用程序在硬件中使用位置功能，例如：geofencing api。
android.permission.MANAGE_DOCUMENTS	签名	允许管理文档访问，通常在选择器中	允许应用程序管理对文档的访问，通常作为文档选取器的一部分。
android.permission.MANAGE_MEDIA	签名	允许修改和删除媒体文件而无需用户确认	允许应用程序修改和删除此设备或任何连接的存储设备上的媒体文件，而无需用户确认。
android.permission.MANAGE_ONGOING_CALLS	签名	查询和管理正在进行的通话详细信息	允许查询正在进行的通话详情和管理正在进行的通话。
android.permission.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。

android.permission.MASTER_CLEAR	签名(系统)	恢复出厂设置	允许应用程序将系统恢复为出厂设置，即清除所有数据、配置以及所安装的应用程序。
android.permission.MEDIA_CONTENT_CONTROL	普通	允许控制媒体内容播放	允许一个应用程序知道什么是播放和控制其内容。
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.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。
android.permission.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储设备	允许应用程序格式化可移除的存储设备。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.NFC_PREFERRED_PAYMENT_INFO	普通	允许接收 NFC 首选支付服务信息	允许应用程序接收NFC首选支付服务信息。
android.permission.NFC_TRANSACTION_EVENT	普通	允许接收 NFC 交易事件	允许应用程序接收 NFC 交易事件。
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.PERSISTENT_ACTIVITY	危险	让应用程序始终运行	允许应用程序部分持续运行，这样系统便不能将其用于其他应用程序。
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、另行转接甚至阻止外拨电话。
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.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.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.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.READ_INPUT_STATE	签名	记录您键入的内容和执行的操作	允许应用程序查看您按的键，即使在与其他应用程序交互（例如输入密码）时也不例外。普通应用程序从不需要使用此权限。
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.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.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.READ_PRECISE_PHONE_STATE	危险	允许以只读方式访问精确的电话状态	允许只读访问精确的电话状态。允许读取特殊用途应用程序（如拨号器、运营商应用程序或ims应用程序）的电话状态详细信息。
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.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_SYNC_STATS	普通	读取同步统计信息	允许应用程序读取同步统计信息；例如已发生的同步历史记录。
com.android.voicemail.permission.READ_VOICEMAIL	未知	未知权限	来自 android 引用的未知权限。
android.permission.REBOOT	签名(系统)	强行重新启动手机	允许应用程序强行重新启动手机。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
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。
android.permission.RECEIVE_WAP_PUSH	危险	接收WAP	允许应用程序接收和处理 WAP 信息。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.REQUEST_COMPANION_PROFILE_WATCH	普通	允许与“手表”设备关联	CompanionDeviceManager 允许应用通过作为“手表” 请求与设备关联。
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_START_FOREGROUND_SERVICES_FROM_BACKGROUND	普通	允许配套应用程序从后台启动前台服务	允许配套应用从后台启动前台服务。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.REQUEST_OBSERVE_COMPANION_DEVICE_PRESENCE	普通	允许订阅配套设备存在状态通知	允许应用程序订阅有关其关联配套设备的在线状态更改的通知，API 31新增。
android.permission.REQUEST_PASSWORD_COMPLEXITY	普通	允许请求和提示屏幕锁定复杂性升级	允许应用程序请求屏幕锁定复杂度并提示用户将屏幕锁定更新到一定的复杂度级别。
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.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.SEND_RESPOND_VIA_MESSAGE	签名(系统)	允许在通话期间发送通过消息响应的请求	允许应用程序（电话）向其他应用程序发送请求，以在传入呼叫期间处理通过消息响应操作。

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。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
android.permission.SET_ALWAYS_FINISH	危险	关闭所有后台应用	允许应用程序控制活动是否始终是一转至后台就完成。普通应用程序从不需要使用此权限。
android.permission.SET_ANIMATION_SCALE	危险	修改全局动画速度	允许应用程序随时更改全局动画速度（加快或放慢动画）。
android.permission.SET_DEBUG_APP	危险	启用应用程序调试	允许应用程序启动对其他应用程序的调试。恶意应用程序可借此终止其他应用程序。
android.permission.SET_PREFERRED_APPLICATIONS	签名	设置首选应用程序	允许应用程序修改首选的应用程序。这样恶意应用程序可能会暗中更改运行的应用程序，从而骗过您现有应用程序来收集您的保密数据。
android.permission.SET_PROCESS_LIMIT	危险	限制运行的进程个数	允许应用程序控制要运行的进程数上限。普通应用程序从不需要使用此权限。
android.permission.SET_TIME	签名(系统)	设置时间	允许应用程序更改手机的时间。
android.permission.SET_TIME_ZONE	危险	设置时区	允许应用程序设置时区。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
android.permission.SET_WALLPAPER_HINTS	普通	设置壁纸大小	允许应用程序设置壁纸大小。
android.permission.SIGNAL_PERSISTENT_PROCESSES	危险	发送Linux信号	允许应用程序请求将所提供的信号发送给所有持久进程
android.permission.SMS_FINANCIAL_TRANSACTIONS	签名	允许金融应用读取过滤后的短信	允许金融应用阅读过滤短信，此权限在 API 级别 31 中已弃用。
android.permission.START_FOREGROUND_SERVICES_FROM_BACKGROUND	普通	从后台启动前台服务	允许应用程序随时从后台启动前台服务，API 31新增。
android.permission.START_VIEW_PERMISSION_USAGE	签名	允许启动应用程序的权限使用屏幕	允许持有者启动应用程序的权限使用屏幕。
android.permission.STATUS_BAR	签名(系统)	修改/禁止状态条	允许应用打开、关闭、禁用状态栏和图标。对第三方应用不可用。
android.permission.TRANSMIT_IR	普通	允许使用设备的红外发射器	允许使用设备的红外发射器（如果可用）。
android.permission.UPDATE_DEVICE_STATS	签名(系统)	更新设备状态	允许应用程序更新设备状态。
android.permission.UPDATE_PACKAGES_WITHOUT_USER_ACTION	普通	允许更新包而不需要用户操作	允许应用程序通过 PackageInstaller.SessionParams.setRequireUserAction(int) 该用户操作指示应用程序更新不需要。
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.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
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
android.permission.USE_ICC_AUTH_WITH_DEVICE_IDENTIFIER	签名	允许读取设备标识符并使用基于 ICC 的身份验证	允许读取设备标识符并使用基于ICC的身份验证，如EAP-AKA。 在身份验证中通常需要访问运营商的服务器并管理订户的服务。

android.permission.USE_SIP	危险	收听/发出网络电话	允许应用程序使用SIP服务拨打接听互联网通话。
android.permission.UWB_RANGING	危险	使用超宽带对设备进行测距所需	需要能够使用超宽带覆盖设备。
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.WRITE_APN_SETTINGS	危险	写入访问点名称设置	允许应用程序写入访问点名称设置。
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_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.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.WRITE_GSERVICES	签名(系统)	修改Google服务地图	允许应用程序修改谷歌地图服务。
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.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_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
com.android.voicemail.permission.WRITE_VOICEMAIL	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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。
com.termux.permission.RUN_COMMAND	未知	未知权限	来自 android 引用的未知权限。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

MANIFEST分析

高危: **1** | 警告: **3** | 信息: **0** | 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	Activity (com.stardust.auojs.inrt.SplashActivity) 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="") 来修复漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
3	Activity设置了TaskAffinity属性 (com.stardust.autojs.core.permission.PermissionRequestActivity)	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设置了TaskAffinity属性 (com.stardust.autojs.core.image.capture.ScreenCaptureRequestActivity)	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

安全漏洞检测

高危: **2** | 警告: **10** | 信息: **2** | 安全: **1** | 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	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
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	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

5	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
6	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
7	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
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	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
10	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	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	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
13	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

14	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
15	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

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/libjackpal-androidterm5.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。	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。	True info 符号被剥离
2	arm64-v8a/libjackpal-termexec2.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。	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	True info 符号被剥离

行为分析

编号	行为	标签	文件
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	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

00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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
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
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
00045	查询当前运行的应用程序名称	信息收集 反射	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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
00191	获取短信收件箱中的消息	短信	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
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
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	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
00123	连接到远程服务器后将响应保存为 JSON	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
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限

00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	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
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00167	使用辅助功能服务执行在活动窗口中获取 root 的操作	无障碍服务	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	29/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.ACCEPT_HANDOVER android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.PACKAGE_USAGE_STATS android.permission.PROCESS_OUTGOING_CALLS android.permission.READ_CALENDAR android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.RECEIVE_MMS android.permission.RECEIVE_SMS android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_CALENDAR android.permission.WRITE_CALL_LOG android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS

其它常用权限	31/46	android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_CHECKIN_PROPERTIES android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_NOTIFICATION_POLICY android.permission.ACCOUNT_MANAGER android.permission.ACTIVITY_RECOGNITION android.permission.BATTERY_STATS android.permission.BIND_APPWIDGET android.permission.BIND_DEVICE_ADMIN android.permission.BIND_INPUT_METHOD android.permission.BIND_REMOTEVIEWS android.permission.BIND_WALLPAPER android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.BROADCAST_PACKAGE_REMOVED android.permission.BROADCAST_SMS android.permission.BROADCAST_STICKY android.permission.BROADCAST_WAP_PUSH android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.DIAGNOSTIC android.permission.MOUNT_FORMAT_FILESYSTEMS android.permission.REORDER_TASKS

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
mk.autoxjs.com	安全	是	**IP地址:** 120.25.164.233 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://github.com/lodash/lodash.git • https://mdn.io/Array/reverse • https://html.spec.whatwg.org/multipage/form-elements.html • https://lodash.com/icon.svg • https://bugzilla.mozilla.org/show_bug.cgi?id=695438 • https://dom.spec.whatwg.org • https://github.com/feross/buffer/issues/166	

- https://img.shields.io/npm/v/bluebird-co.svg?style=flat
- https://github.com/lodash/lodash/blob/4.17.15/dist/lodash.js
- http://goo.gl/rRqMUw
- https://github.com/tc39/proposal-shadowrealm/pull/384
- http://xv.mingshengsheng.com
- https://img.shields.io/npm/l/bluebird-co.svg?style=flat
- https://mdn.io/Number/isInteger
- http://peter.michaux.ca/articles/lazy-function-definition-pattern
- http://qn2404.ysqyy.top/xvauto/ids/version.json?v=
- https://travis-ci.org/novacrazy/bluebird-co.svg?branch=master
- http://qn2404.ysqyy.top/xvauto/tips/comment_date_tips.jpg
- https://github.com/fb55/css-select/pull/43
- https://has1.dcloud.net.cn/ahl
- https://github.com/sindresorhus/p-is-promise/blob/cda35a513bda03f977ad5cde3a079d237e82d7ef/index.js
- https://github.com/nodejs/node/commit/112cc7c27551254aa2b17098fb774867f05ed0d9
- http://babeljs.io/docs/plugins/transform-async-to-module-method/
- https://feross.org/opensource
- https://goo.gl/t5IS6M
- http://qn2404.ysqyy.top/xvauto/tips/comment_tips.jpg
- https://github.com/petkaantonov/bluebird
- http://qn2404.ysqyy.top/xvauto/tips/comment_content_tips.jpg
- https://travis-ci.org/lodash/lodash/
- https://github.com/lodash/lodash/tree/4.17.21-npm
- http://qn2404.ysqyy.top/xvauto/tips/like_tips.jpg
- http://mathiasbynens.be/notes/javascript-encoding
- https://github.com/nodejs/node/blob/v10.8.0/lib/internal/errors.js
- https://github.com/mafintosh/pump
- https://lodash.com/custom-builds
- http://requirejs.org/docs/errors.html
- https://github.com/zloirock/core-js/blob/v3.36.1/LICENSE
- https://html.spec.whatwg.org/multipage/semantics-other.html
- http://www.whatwg.org/specs/web-apps/current-work/multipage/parsing.html
- https://mathiasbynens.be/notes/javascript-unicode
- http://bluebirdjs.com/docs/api-reference.html
- http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd
- http://wonko.com/post/html-escaping
- https://mdn.io/toUpperCase
- https://fontawesome.com/license/free
- https://mdn.io/Number/isFinite
- https://github.com/lodash/lodash
- https://api.next.bspapp.com
- https://github.com/slevithan/xregexp/blob/95eeebeb8fac8754d54eafe2b4743661ac1cf028/src/xregexp.js
- https://github.com/bnjmnt4n/lodash-cli.git
- https://mths.be/he
- http://underscorejs.org/LICENSE
- http://qn2404.ysqyy.top/xvauto/tips/collection_tips.jpg
- http://goo.gl/MqrmXu000au000a
- http://qn2404.ysqyy.top/xvauto/tips/comment_like_tips.jpg
- https://github.com/beatgammit/base64-js/issues/42
- http://www.ecma-international.org/ecma-262/7.0/
- https://mdn.io/rest_parameters
- https://github.com/fb55/boolbase
- https://lodash.com/
- https://github.com/TypeStrong/typedoc/issues/1616
- https://github.com/mafintosh/end-of-stream
- https://github.com/novacrazy/bluebird-co/tree/master/benchmark
- https://mdn.io/isNaN
- http://www.ecma-international.org/ecma-262/7.0/
- https://api.bspapp.com
- https://css-tricks.com/debouncing-throttling-explained-examples/
- https://mdn.io/clearTimeout
- http://www.whatwg.org/specs/web-apps/current-work/multipage/tree-construction.html
- https://github.com/feross/buffer/pull/148

自研引擎-A

- http://ejohn.org/blog/javascript-micro-templating/
- http://qn2404.ysqyy.top/xvauto/ids/gifmaker.json?v=
- http://bluebirdjs.com/docs/api/promise.coroutine.addyieldhandler.html
- https://github.com/feross/buffer/issues/154
- https://mdn.io/Array/slice
- https://www.baidu.com
- http://qn2404.ysqyy.top/xvauto/tips/title_tips.jpg
- https://mdn.io/setTimeout
- https://github.com/jashkenas/underscore/pull/1247
- https://github.com/zloirock/core-js
- http://goo.gl/MqrFmXu000a
- https://html.spec.whatwg.org/multipage/scripting.html
- http://qn2404.ysqyy.top/xvauto/tips/desc_tips.jpg
- http://creativecommons.org/publicdomain/zero/1.0/
- http://qn2404.ysqyy.top/xvauto/ids/community.json?v=
- https://github.com/feross/buffer/issues/219
- https://mdn.io/String/replace
- https://feross.org
- https://mdn.io/Object/assign
- http://qn2404.ysqyy.top/xvauto/tips/input_tips.jpg
- https://github.com/tj/co/blob/master/Readme.md
- https://mdn.io/Number/isSafeInteger
- https://openjsf.org/
- https://dom.spec.whatwg.org/
- https://img.shields.io/npm/dm/bluebird-co.svg?style=flat
- http://www.html5rocks.com/en/tutorials/developertools/sourcemaps/
- https://github.com/olado/doT
- https://github.com/WebReflection/get-own-property-symbols/issues/4
- https://mdn.io/round
- https://fontawesome.comn
- https://uri.amap.com/navigation?
- http://javascript.crockford.com/jsmin.html
- http://qn2404.ysqyy.top/xvauto/tips/comment_area_tips.jpg
- https://mdn.io/Structured_clone_algorithm
- https://mdn.io/spread_operator
- http://eev.ee/blog/2015/09/12/dark-corners-of-unicode/
- https://developer.chrome.com/extensions/sandboxingEval
- https://github.com/pkaminski
- http://qn2404.ysqyy.top/xvauto/tips/follow_tips.png.jpg
- http://stackoverflow.com/a/22747272/680742
- https://mdn.io/Number/isNaN
- https://github.com/novacrazy/bluebird-co/issues
- https://cheerio.js.org
- http://qn2404.ysqyy.top/xvauto/tips/collection_emoji.jpg
- https://github.com/ljharb/object.assign/issues/17
- https://github.com/novacrazy/bluebird-co
- https://github.com/mathiasbynens/he/blob/36afe179392226cf1b6ccdb16ebbb7a5a844d93a/src/he.js
- https://github.com/tj/co/issues/180
- https://mdn.io/toLowerCase
- https://npmjs.org/package/bluebird-co
- http://underscorejs.org/
- http://qn2404.ysqyy.top/xvauto/ids/douyin.json?v=
- http://dom.spec.whatwg.org/
- https://travis-ci.org/lodash-archive/lodash-cli
- https://lodash.com/license
- https://hac1.dcloud.net.cn/ah5
- https://github.com/zloirock/core-js/blob/v3.26.1/LICENSE
- https://html.spec.whatwg.org/multipage/parsing.html
- https://mathiasbynens.be/notes/ambiguous-ampersands
- http://bluebirdjs.com/docs/api/promise.coroutine.html
- https://mdn.io/iteration_protocols
- https://travis-ci.org/novacrazy/bluebird-co
- https://mdn.io/String/split
- https://saucelabs.com/u/lodash

• https://github.com/tj/co	
• http://120.25.164.233:8080/appstore/app/checkversion?id=22	com/stardust/auojs/inrt/util/UpdateUtil.java
• http://mk.autoxjs.com/pages/ykapp/choisefeature	com/stardust/auojs/inrt/FeatureActivity.java
• 112.74.161.35	com/stardust/auojs/inrt/SplashActivity$onCreate$1.java
• http://127.0.0.1	com/stardust/autojs/rhino/debug/Dim.java
• file:/android_asset/modules • file:/android_asset/ • file:/android_asset/modules/npm • file:/android_asset	com/stardust/autojs/engine/module/AssetAndUrlModuleSourceProvider.java
• https://github.com/vinc3m1/roundedimageview • http://jackpal.github.com/android-terminal-emulator/help/index.html • https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
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。
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

密钥凭证

可能的密钥
"key_enable_accessibility_service_by_root" : "key_enable_accessibility_service_by_root"
"key_dont_show_main_activity" : "key_dont_show_main_activity"
"pref_controlkey_default" : "5"
"key_enable_floating_window" : "key_enable_floating_window"
"key_enable_accessibility_service" : "key_enable_accessibility_service"
"key_stable_mode" : "key_stable_mode"

"special_keys" : "Spezialtasten"
"key_print_java_stack_trace" : "key_print_java_stack_trace"
"key_use_volume_control_running" : "key_use_volume_control_running"
"pref_fnkey_default" : "4"
"key_keep_running_with_foreground_service" : "key_keep_running_with_foreground_service"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

免责声明及风险提示: