南明离火
——移动应用检测平台——

ANDROID 静态分析报告

新网格通 • v5.2.6

分析日期: 2024-07-03 11:38:31

应用概览

文件名称:	WGT-5.2.6-20240620_release_20240627120241_sec.apk
文件大小:	94.96MB
应用名称:	新网格通
软件包名:	com.huawei.ado.jiangxi.wgt
主活动:	com.huawei.ado.pocket.splashscreen.SplashScreenActivity
版本号:	5.2.6
最小SDK:	24
目标SDK:	33
加固信息:	梆梆安全（企业版）加固
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	881b3fd4840609dbe458b60ef0831e92
SHA1:	f64c63b94e0d09baca489bbef7e478618418cef4
SHA256:	148f3e54fc7e307bd79c05de065a647eb183c6156951e03e4b673437e9f73291

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
2	4	0	1	0

四大组件导出状态统计

Activity组件：130个，其中export的有： 2个
Service组件：7个，其中export的有： 0个
Receiver组件：2个，其中export的有： 0个
Provider组件：11个，其中export的有： 0个

应用签名证书信息

二进制文件没有签名
缺少代码签名证书
v1 签名: False
v2 签名: False
v3 签名: False
v4 签名: False

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.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.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.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.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.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.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_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.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_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.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.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.HIDE_NON_SYSTEM_OVERLAY_WINDOWS	未知	未知权限	来自 android 引用的未知权限。

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.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.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。
com.asiainfo.cm10085.IDENTITY_AUTHENTICATION	未知	未知权限	来自 android 引用的未知权限。
MediaStore.Images.Media.INTERNAL_CONTENT_URI	未知	未知权限	来自 android 引用的未知权限。
MediaStore.Images.Media.EXTERNAL_CONTENT_URI	未知	未知权限	来自 android 引用的未知权限。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
com.huawei.ado.jiangxi.wgt.permission.INCOMING_CALL	未知	未知权限	来自 android 引用的未知权限。
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）
com.huawei.ado.jiangxi.wgt.com.cmos.sdk.permissions.CUSTOMBROADCAST	未知	未知权限	来自 android 引用的未知权限。
com.huawei.ado.jiangxi.wgt.adom.permission.process.sync	未知	未知权限	来自 android 引用的未知权限。
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
com.huawei.ado.jiangxi.wgt.permission.process.sync	未知	未知权限	来自 android 引用的未知权限。
com.huawei.ado.jiangxi.wgt.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT

com.huawei.ado.pocket.splashscreen.SplashScreenActivity	Schemes: pushscheme://, ado://, Hosts: com.huawei.ado.jiangxi.wgt, com.huawei.nis.android.gridbee, sso.huawei.com, open.huawei.com, Mime Types: text/*, Paths: /deeplink, Path Prefixes: /web, /main, /,

网络通信安全风险分析

高危: **1** | 警告: **0** | 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。

证书安全合规分析

高危: **1** | 警告: **0** | 信息: **0**

标题	严重程度	描述信息
缺少代码签名证书	高危	未找到代码签名证书

Manifest 配置安全分析

高危: **0** | 警告: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 7.0, [minSdk=24]	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。
4	Activity (com.alipay.sdk.app.PayResultActivity) 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。
5	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。

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)	SYMBOLSSTRIPPED(裁剪符号表)

1	arm64-v8a/libcmos.so	False high 二进制文件没有设置NX位。NX位可以通过将内存页标记为不可执行来防止内存损坏漏洞被利用。使用选项-noexecstack或-z noexecstack来将栈标记为不可执行		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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项-z,relro,-z,now启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

2	arm64-v8a/libECMedia.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', '__strchr_chk', '__read_chk', '__memcpy_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk']	False warning 符号可用

3	arm64-v8a/libserphone.so	False high 二进制文件没有设置NX位。NX位可以通过将内存页标记为不可执行来防止内存损坏漏洞被利用。使用选项-noexecstack或-z noexecstack来将栈标记为不可执行		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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项-z,relro,-z,now启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	10/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.VIBRATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE
其它常用权限	12/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.BLUETOOTH android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息

journeyapps.com	安全	否	**IP地址:** 13.225.131.83 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
www.videolan.org	安全	否	**IP地址:** 213.36.253.2 **国家:** 法国 **地区:** 法兰西岛 **城市:** 巴黎 **纬度:** 48.859077 **经度:** 2.293486 **查看:** Google 地图
tools.ietf.org	安全	否	**IP地址:** 104.16.45.99 **国家:** 美利坚合众国 **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.ietf.org	安全	否	**IP地址:** 104.16.45.99 **国家:** 美利坚合众国 **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

URL 链接安全分析

URL信息	源码文件
• https://www.gneec.com/ • https://github.com/adobe-type-tools/cmap-resources • https://wap.cmpassport.com/resources/html/contract.html	自研引擎-A

• https://github.com/journeyapps/zxing-android-embedded • https://journeyapps.com/	自研引擎-S
• 127.0.0.1 • http://www.videolan.org/x264opt.html • http://tools.ietf.org/html/draft-ietf-avtext-framemarking-07 • 3.0.16.9 • http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 • 8.8.8.8	lib/arm64-v8a/libECMedia.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
梆梆安全	梆梆安全	针对目前移动应用普遍存在的破解、篡改、盗版、钓鱼欺诈、内存调试、数据窃取等各类安全风险，梆梆安全为开发者提供全面的移动应用加固加密技术和攻击防范服务。
OpenSSL	OpenSSL	OpenSSL 是用于传输层安全性协议（TLS）和安全套接字层（SSL）协议的功能强大的，商业级且功能齐全的工具包。
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
SQLite	SQLite	SQLite 是遵守 ACID 的关系数据库管理系统，它包含在一个相对小的 C 程序库中。与许多其它数据库管理系统不同， SQLite 不是一个客户端/服务器结构的数据库引擎，而是被集成在用户程序中。 SQLite 遵守 ACID ，实现了大多数 SQL 标准。它使用动态的、弱类型的 SQL 语法。

邮箱地址敏感信息提取

EMAIL	源码文件
ado@huawei.com	自研引擎-S

敏感凭证泄露检测

可能的密钥
"pwd_expire_dialog_cancel" : "Later"
"fill_info_person_password" : "Parola"
"fill_info_person_password" : "Password"
"library_zxingandroidembedded_author" : "JourneyApps"
"login_pwd" : "Password"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。