南明离火
移动应用检测平台

ANDROID 静态分析报告

谷歌浏览器 • v2.0.0.0

分析日期: 2025-07-06 20:42:15

应用概览

文件名称:	谷歌浏览器.apk
文件大小:	20.62MB
应用名称:	谷歌浏览器
软件包名:	ahc11.fwm75.f66po
主活动:	ahc11.fwm75.f66po.HomeShow.HomeStartShowActivity
版本号:	2.0.0.0
最小SDK:	21
目标SDK:	35
加固信息:	自定义加固
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	2/432
杀软检测:	20 个杀毒软件报毒
MD5:	4c37f54cdbe921c00e882b39c11c14c8
SHA1:	6439d0b57209e2ee5c82d945f4912b961e3f5024
SHA256:	deeb55394d05aef38fecd2c2ad3bff40ce45752bfecb489ebf3503b208d1f3bd

分析结果严重性分布

高危	中危	信息	安全	关注
2	43	2	0	8

四大组件导出状态统计

Activity组件：32个，其中export的有： 12个
Service组件：10个，其中export的有： 7个
Receiver组件：13个，其中export的有： 6个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=admind0oqvp, ST=admind0oqvp, L=admind0oqvp, O=admind0oqvp, OU=admind0oqvp, CN=admind0oqvp
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-15 22:49:59+00:00
有效期至: 2125-05-22 22:49:59+00:00
发行人: C=admind0oqvp, ST=admind0oqvp, L=admind0oqvp, O=admind0oqvp, OU=admind0oqvp, CN=admind0oqvp
序列号: 0xa3798b3
哈希算法: sha256
证书MD5: 88ee3ce47b5a1484b8e651e6a3b671b6
证书SHA1: 4fa220002e2e0a3546d7782f8fa67f78752dad82
证书SHA256: 71ec5d4c92df5f930d17e5b419a21263033ac72e5d77ed646f645b184a5d60ce
证书SHA512:
993c3063ea704196c40550716d0f319b8fe551b25d28b02783040e77e5c1666fed258bffc4c3d7c43[illegible]87[illegible]b0e83a02c9112473[illegible]1ac8ce75d97df14a81c

公钥算法: rsa
密钥长度: 1024
指纹: aa4d3d61e22384dedee73ef032153f2749e75fdac27798bbe2fe3383217e4[illegible]
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.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.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_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.lclient.Main.permission.RECEIVE_MSG	未知	未知权限	来自 android 引用的未知权限。
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.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.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.MOUNT_UNMOUNT_FILESYSTEM	未知	未知权限	来自 android 引用的未知权限。
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.USE_EXACT_ALARM	普通	允许在未经用户许可的情况下使用精确的警报	允许应用使用精确的警报。
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.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_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.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.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.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.INTERNAL_SYSTEM_WINDOW	签名	显示未授权的窗口	允许创建专用于内部系统用户界面的窗口。普通应用程序不能使用此权限。
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_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.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.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.DEVICE_POWER	签名	开机或关机	允许应用程序启动/关闭设备。
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.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.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.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.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.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.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.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.FORCE_STOP_PACKAGES	签名	强行停止其他应用程序	允许应用程序强行停止其他应用程序。
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.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.FOREGROUND_SERVICE_MEDIA_PROJECTION	普通	允许媒体投影的前台服务	允许常规应用程序使用类型为“mediaProjection”的 Service.startForeground。
android.permission.CAPTURE_VIDEO_OUTPUT	普通	允许捕获视频输出	允许应用程序捕获视频输出。
android.permission.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
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.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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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_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.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.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.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.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.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。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **33** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Activity-Alias (ahc11.fwm75.f6bpo.tqActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。

3	Activity-Alias (ahc11.fwm75.f66po.androidActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (ahc11.fwm75.f66po.HomeShow.HomeMainShowActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Activity (ahc11.fwm75.f66po.HomeShow.VerifyLogShowActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (ahc11.fwm75.f66po.HomeShow.AutoScreenShowActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (ahc11.fwm75.f66po.HomeShow.Acitivity1) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity-Alias (ahc11.fwm75.f66po.FestivalActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
9	Activity-Alias (ahc11.fwm75.f66po.MainAliasActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
10	Activity (ahc11.fwm75.f66po.HomeShow.OpenShow_Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (ahc11.fwm75.f66po.HomeShow.show1_Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
12	Activity (ahc11.fwm75.f66po.HomeShow.show2_Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
13	Activity (ahc11.fwm75.f66po.HomeShow.show3_Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Broadcast Receiver (ahc11.fwm75.f66po.backs.SelfStartRunUse) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

15	Service (ahc11.fwm75.f66po.backs.BackRunServerUseUse) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
16	Service (ahc11.fwm75.f66po.backs.ScreenServer) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
17	Service (ahc11.fwm75.f66po.backs.BackAccessRunServiceUseUse) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
18	Service (ahc11.fwm75.f66po.backs.MessageToolUse) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
19	Broadcast Receiver (ahc11.fwm75.f66po.backs.NumberStateBr) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
20	Service (com.baidu.location.f) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
21	Broadcast Receiver (ahc11.fwm75.f66po.backs.DelayBrUse) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
22	Broadcast Receiver (ahc11.fwm75.f66po.backs.AlarmUtils_BrUse_Utils) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
23	Broadcast Receiver (ahc11.fwm75.f66po.backs.CloseBlackAlarmUtils) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

24	Service (ahc11.fwm75.f66po.backs.MyService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
25	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
26	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
27	检测到拨号暗码：123321 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
28	检测到拨号暗码：735564 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
29	检测到拨号暗码：787878 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
30	检测到拨号暗码：898989 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
31	检测到拨号暗码：565656 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
32	检测到拨号暗码：656565 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。
33	检测到拨号暗码：123456 [android:scheme="android_secret_code"]	警告	Manifest 中存在拨号暗码（如：*#*#4636#*#*），输入后可触发隐藏功能，存在敏感信息泄露风险。

代码安全漏洞检测

高危: **2** | 警告: **8** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
4	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
5	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
6	该文件是World Writable。任何应用程序都可以写入文件	高危	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
7	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
8	该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

9	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
10	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
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	使用弱加密算法	高危	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libcrypto-utils.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，以便它在被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

2	arm64-v8a/libnmmp.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
3	arm64-v8a/libUtils.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

4	arm64-v8a/libYuvOsd.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	False warning 符号可用

应用行为分析

编号	行为	标签	文件
00056	修改语音音量	控制	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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00106	获取当前格式化的WiFi的IP地址	信息收集 WiFi	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
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
00134	获取当前WiFi IP地址	WiFi 信息收集	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

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
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
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
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
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
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
00168	使用辅助服务执行全局操作，通过文本获取节点信息	无障碍服务	升级会员：解锁高级权限
00169	使用辅助服务执行全局操作，通过视图 ID 获取节点信息	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
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
00189	获取短信内容	短信	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
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

00035	查询已安装的包列表	反射	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
00044	查询该包的activity上次被使用的时间	信息收集 反射	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
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
00036	从 res/raw 目录获取资源文件	反射	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
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
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
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
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
00208	捕获设备屏幕的内容	信息收集 屏幕	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
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00006	安排录制任务	录制音视频	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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	21/30	android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE android.permission.ACCESS_FINE_LOCATION android.permission.WRITE_SETTINGS android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.PACKAGE_USAGE_STATS android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_CALL_LOG android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS
其它常用权限	12/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.FORCE_STOP_PACKAGES android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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

whois.pconline.com.cn	安全	是	**IP地址:** 119.23.148.22 国家: 中国 地区: 江苏 城市: 苏州 纬度: 31.311365 经度: 120.617691 查看: 高德地图
www.raylink.live	安全	是	**IP地址:** 119.23.148.22 国家: 中国 地区: 江苏 城市: 常州 纬度: 31.783331 经度: 119.966667 查看: 高德地图
sunlogin.oray.com	安全	是	**IP地址:** 119.23.148.22 国家: 中国 地区: 江苏 城市: 无锡 纬度: 31.569349 经度: 120.288738 查看: 高德地图
www.envcom.org	安全	否	**IP地址:** 104.21.41.99 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
admin.saas.360.cn	安全	是	**IP地址:** 119.23.148.22 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
www.kuaijiexi.com	安全	是	**IP地址:** 119.23.148.22 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
software.airmore.cn	安全	是	**IP地址:** 119.23.148.22 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

www.hgzvip.net	安全	是	**IP地址:** 119.23.148.22 **国家:** 中国 **地区:** 江苏 **城市:** 连云港 **纬度:** 34.600025 **经度:** 119.166847 **查看:** 高德地图
www.myweb.com	安全	否	**IP地址:** 50.6.160.92 **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
hsk.oray.com	安全	是	**IP地址:** 221.228.217.236 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288738 **查看:** 高德地图
checkip.amazonaws.com	安全	否	**IP地址:** 34.203.60.120 **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

URL 链接安全分析

URL信息	源码文件
• ws://%s:8081/websocket?userid=	ahc11/fwm75/f66po/backs/BackRunServerUseUse.java
• file:allx	ahc11/fwm75/f66po/HomeShow/HomeMainShowActivity.java
• https://www.anysdk.org/h5/#/page/u1/d1	ahc11/fwm75/f66po/HomeShow/HomeMainShowActivity$3.java

• http://whois.pconline.com.cn/ipjson.jsp?ip=%s&json=true • https://www.raylink.live/?utm_source=bdsem&utm_group=gjc&utm_term=%d4%b6%b3%cc%bf%d8%d6%c6&utm_device=pc-cpc&e_matchtype=1&e_creative=72696644698&e_adposition=cl2&e_keywordid=610500548200&e_keywordid2=610500548200&bd_vid=8448251558619904973 • https://www.hgzvip.net/ • https://hsk.oray.com/download/?utm_source=baidu&utm_medium=cpc&utm_campaign=hsk_download&referral_id=47020&wordid=pc01009007520230725000151&adp=cl2&bd_vid=9248793334743568588 • http://%s:8082/imcenter/imgroupcontroller/insert • http://%s:8082/imcenter/imgroupcontroller/removeuser • http://%s:8082/imcenter/imgroupcontroller/adduser • https://sunlogin.oray.com/ • https://www.kuaijiexi.com/?user_from=baidu_sem&keyword=ngrok%d4%b6%b3%cc%d7%c0%c3%e6&bd_vid=9925315598383029393 • http://www.myweb.com/ • https://software.airmore.cn/apowermirror?apptype=aps-bd&bd_vid=8726690745186985370 • https://checkip.amazonaws.com/ • http://%s:8082/imcenter/imgroupcontroller/updatebyid • https://admin.saas.360.cn/login	ahc11/fwm75/f66po/SetTool/ToolUse/ConfigDataSetUse/HttpStateUseTool.java
• http://play.google.com/store/apps/details?id=	ahc11/fwm75/f66po/SetTool/ToolUse/ConfigDataSetUse/IMyUseTool.java
• http://%s:8090	ahc11/fwm75/f66po/SetTool/ToolUse/LogToolUse/UrlKey.java
• https://www.baidu.com • www.baidu.com • http://www.baidu.com	ahc11/fwm75/f66po/SetTool/ToolUse/PurposeUse/NetUseUtils.java
• https://www.baidu.com/	ahc11/fwm75/f66po/SetTool/ToolUse/PurposeUse/SpFunSet.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
WebRTC	WebRTC	借助 WebRTC，您可以在基于开放标准的应用程序中添加实时通信功能。它支持在同级之间发送视频，语音和通用数据，从而使开发人员能够构建功能强大的语音和视频通信解决方案。该技术可在所有现代浏览器以及所有主要平台的本机客户端上使用。 WebRTC 背后的技术被实现为一个开放的 Web 标准，并在所有主要浏览器中均以常规 JavaScript API 的形式提供。
nmmp	nmcabc	nmmp 是一个用于保护 Android 类的 dex 文件的库，它使用 dex-vm 技术将类和方法转换为字节码，从而防止反编译。
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
loc-bugs@baidu.com	ahc11/fwm75/f66po/SetTool/Placebd/LocationCoordUseSe.java

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99

敏感凭证泄露检测

可能的密钥
x5bHlMSTx5xkxIcgY29udGV4dDrHnGTEh8eWY8SV
w7zun4jEh8ecZMSHRGVsZWdhdGVBcHBsaWNhdGlvbi5vbkNyZWF0ZTLHnGTEh8O8w7zEiQ==
ZWXEhcecZMSHYW5kcm9pZC5hcHAuTG9hZ2VyQXBrx5xkxIfHmMOCxic=
Y2bEicecZMSHPT09PT0+cmVwYXBwLx5xkxIfun4jHnMSL
Y8O5xJFlY8SNZ2V0QXBwbGljYXRpb25jbmZvZWPEjcO8ZcSR
Y2TEg8ecZMSHb25DcnVldGVneDI6x5xkxIfHmGbcrcO=
w7rFq8SDZWPEjTQ0NDQ0NDQ0NGVjxI1mx5zFgw==
7p+IZsSFx5xkxIdnZXRJbnN0YW5jZreSZMSHx5rFq8SR
ZWbEg8ecZMSHbVByb3ZpZGVyTWFwx5xkxIdjY8SF
x5bDvMSLZMecxIMgdXx8dVklTSUJMRWTHnMSDw7zFq8SN
x5zHlsSFZMecxINzcGVjaWFsRWZmZWN0c0NvbnRyb2xsZXI6IFNldHRpbmcgdmlldyBkx5zEg8eWw7zEhw==
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
ZsO5xInHnGTEh2F0dGFjaMecZMSHw7xjxIs=
w7zHlMSNx5xkxIdvbkNyZWF0ZUV4NMecZMSHx5jDusSP

w7xjxJHHnGTEhyBmaWxlTmFtZTrHnGTEh8eUx5TEkw==
YsO6xIHHnGTEh21BcHBsaWNhdGlvbsecZMSHw7zHnMSD
xavDusSJZMecxIMgdG8gR09ORWTHnMSDx5zDucSL
pbe8qqrub83wl4475ke6twat2eljzal6km0v6jbvdsmtfash
ZsO5xJHHnGTEh0FFUy9DQkMvUEtDUzVQYWRkaW5nx5xkxIfHlMeYxJM=
YseYxJFkx5zEg1JFTU9WSU5HZMecxINixavEkw==
x5zDucSTx5xkxIdhbmRyb2lkLmFwcC5BY3Rpdml0eVRocmVhZMecZMSHZseYxJU=
Y8O5xIHHnGTEh2N1cnJlbnRBY3Rpdml0eVRocmVhZMecZMSHYceaxIM=
YWLEhcecZMSHbUxvY2FsUHJvdmlkZXLHnGTEh2PHmsSH
w7zFq8SRZMecxINVbmtub3duIHZpc2liaWxpdHkgZMecxINhw7rEkw==
YmbEkcecZMSHb25DcmVhdGVFeDExOsecZMSHY8O5xJM=
WgY90A5kN0xjrvaFf9ovvicXXEiHaSPxvwwOSIRJ2vM=
YWPEj2VjxI1hbmRyb2lkLmNvbnRlbnQucG0uUGFja2FnZU1hbmFnZXJlY8SNw7xiI8=
x5bDucSNx5xkxIdtUGFja2FnZUluZm/HnGTEh2JmxI8=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
x5ZjxI/HnGTEh21Jbml0aWFsQXBwbGljYXRpb27HnGTEh2eWYcSR
YmXEicecZMSHPT09PT0+x5xkxIfDuWPEiw==
uT733U5aSS6ApqQQxF8hM4RpzJC0d/sIaBWkdkYVEhI8=
w7xkxJPHnGTEh21QYWNrYWdlSW5mb8ecZMSHYcO6xJU=
YseWxJHHnGTEh21BcHBsaWNhdGlvbsecZMSHYWLEkw==
w7rHnMSHx5xkxIdhbmRyb2lkLmNvbnRlbnQuQ29udGVudFByb3ZpZGVyx5xkxIfDumLEiQ==
x5jHnMSDx5xkxIdtQXBwbGljYXRpb25Jbm7vx5xkxIdjw7rEhQ==
xavDucSNx5xkxIdvbkNyZWF0ZUV4Mj9cZMSHYe6fiMSN
w7lmxIvHnGTEh3JlcGxhY2VDb25tZW50UHJvdmlkZXIyx5xkxIfHlsO8xI0=
x5THmMSDZMecxINDcUU5UlRVJkx5zEg8eYx5jEhQ==
x5jHmMSPx5xkxIdvbkNyZWF0ZUV4NcecZMSHY2PEkQ==
x5zHnMSNx5xkxIdvbkNyZWF0ZUV4MTrHnGTEh2Tun4jEjw==
w7zFq8SHx5xkxIdhbmRyb2lkLmFwcC5BY3Rpdml0eVRocmVhZMecZMSH7p+IYcSJ
VG/68w3+ZJqFYMuNeUhygA==

x5Tun4jEjcecZMSHbU1haW5UaHJlYWTHnGTEh2VmxI8=
t6gfivdcb27pksoqerj5jm8kqq5fdv0avu
ZsO6xJHHnGTEh21BbGxBcHBsaWNhdGlvbnPHnGTEh2HDvMST
vEQhpTd7MzOeILBbgX4wt0ZgvphmJQbG5iDMEtl0wUknF1xIh2kj8b8MDkiESdrz
ZcWrxI1kx5zEg1NwZWNpYWxFZmZlY3RzQ29udHJvbGxlcjogUmVtb3ZpbmcgdmlldyBkx5zEg8O8w7nEjw==
w7zHlsSJx5xkxIdEZWxlZ2F0ZUFwcGxpY2F0aW9uLm9uQ3JlYXRlMDrHnGTEh2bDusSL
xavDucSFx5xkxIdEZWxlZ2F0ZUFwcGxpY2F0aW9uLm9uQ3JlYXRlMcecZMSHx5zFq8SH
ZMeWxIfHnGTEh3JlcGxhY2VDb250ZW50UHJvdmlkZXIxx5xkxIdlZcSJ
w7rHnMSFZMecxINJTlZJU0lCTEVkx5zEg2JlxIc=
w7zDusSTZMecxINBRERJTkdkx5zEg8WrYsSV
YsecxI/HnGTEh2FuZHJvaWQuYXBwLkxvYWRlZEFwa8ecZMSHw7rDvMSR
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
ZcO6xIvHnGTEh3JlcGxhY2VDb250ZW50UHJvdmlkZXIzx5xkxIfDuWbEjQ==
ZMeUxJVlY8SNMTc1MDA1NjY4NDAwMGVjxI1kw7nEgQ==
ZceYxIFkx5zEg0NFTlRFUl9YZMecxIPDuWPEgw==
YsWrxJNkx5zEg0NFTlRFUl9ZZMecxIPHlmXElQ==
xathxJPHnGTEhyB8IGEuY8ecZMSHx5RhxJU=
xavHmMSNx5xkxIdqYXZheC5jcnlwdG8uQ2lwaGVyx5xkxIfHlsWrxI8=
x5pjxINkx5zEg0ZyYWdtZW50TWFuYWdlcnTHnMSDx5bun4jFhQ==
w7rDvMSBx5xkxIc9PT0+d3JpdGVOaWxlx5xkxIdmw7nEgw==
w7ljxI9kx5zEgyBmcm9tGNlybnRhaW5lciBkx5zEg7rMWrxjE=
Y2bEi8ecZMSHc2V0N3V0ZXJDb250ZXh0x5xkxIfDvMeWxI0=
x5RlxIdkx5zEg0JPVFRPTWTHnMSDxaVFqcSJ

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。