



ANDROID 静态分析报告



连连通WiFi • v1.0

分析日期: 2025-04-30 19:08:13

i应用概览

文件名称:	连连通WiFi v2.1.0.apk
文件大小:	36.55MB
应用名称:	连连通WiFi
软件包名:	com.extolanxio.ban
主活动:	com.ljh.major.module.lauch.SplashActivity
版本号:	2.1.0
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
杀软检测:	2 个杀毒软件报毒
MD5:	ff8514978e8905aa38d59a02bccd29d1
SHA1:	bab17200b3fe729e5ced02e44cf91b35ec8b0d0
SHA256:	84ff182c1eb762a534505b115608a274017722c2f31e76c5939b027d62dc5d64

分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
0	13	1	1	4

四大组件信息

Activity组件: 164个, 其中export的有: 13个
Service组件: 33个, 其中export的有: 9个
Receiver组件: 13个, 其中export的有: 13个
Provider组件: 11个, 其中export的有: 1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=guigangGuangXi, ST=GuangXi, L=guigangGuangXi, O=TanFengLTD, OU=TanFengLTD, CN=TanFengGuiGang
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-29 14:24:20+00:00
有效期至: 2051-04-16 14:24:20+00:00
发行人: C=guigangGuangXi, ST=GuangXi, L=guigangGuangXi, O=TanFengLTD, OU=TanFengLTD, CN=TanFengGuiGang
序列号: 0x2030187d
哈希算法: sha256
证书MD5: dbcb4eecaf44ade830cf592a61df223a
证书SHA1: c674f7a26ebd3a53bb87c4b7c4481b6fe82b86f1
证书SHA256: daa6bbb1a8eed03540eb84af9bdb11b2eb2a473143fdd9296eb3fb29e7551327
证书SHA512:
c401f14b4f0c7fb47efd153bf9a7b6bab9f26704946e7e5ed03abda23505592fa5f89288092e66534bc22321a212a856c8104f136f52b6bfa72e10fe5995ff38

公钥算法: rsa
密钥长度: 2048
指纹: 90e674696bf81ec178b40ee731ddcc185136fdf0fc6121c5c26ec1831504ea3e
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.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.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.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。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，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.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.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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
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.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.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.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.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.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.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。
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
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。
com.extolanxio.ban.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytao.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.extolanxio.ban.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.extolanxio.ban.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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。
com.extolanxio.ban.openadsdk.permission.INTERPA	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.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。
com.ss.android.downloads.permission.ACCESS_PROVIDER	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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

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。
getui.permission.GetuiService.com.extolanxio.ban	未知	未知权限	来自 android 引用的未知权限。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
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。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

可浏览的Activity组件

ACTIVITY	INTENT
com.ljh.major.module.main.MainActivity	Schemes: http://, Hosts: beatmap,
com.ljh.major.router.SchemeFilterActivity	Schemes: xmail://, Hosts: com.ljh.xmail,
com.ljh.major.module.wallpaper.WallPaperAnimActivity	Schemes: wallpaper://, Hosts: anim Ports: 8888, Paths: /show/anim,
com.alipay.sdk.app.AlipayResultActivity	Schemes: com.extolanxio.ban.alipay.result://,

网络通信安全

序号	范围	严重级别	描述
----	----	------	----

证书安全分析

高危: 0 | 警告: 1 | 信息: 0

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: 0 | 警告: 40 | 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.ljh.major.module.main.MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
3	Activity (com.ljh.major.router.SchemeFilterActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
4	Activity (com.extolanxio.ban.wxapi.WXEntryActivity) 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.extolanxio.ban.wxapi.WXPayEntryActivity) 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。
6	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.TrafficRedPacketWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
7	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.WifiLinkWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
8	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.GreenInfoWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
9	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.PacketWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
10	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.RiskWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
11	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.WifiConnectWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。

12	Broadcast Receiver (com.xmbranch.toolwidgets.widgets.GreenPackageWidget) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
13	Service (com.ljh.major.module.wallpaper.LiveWallpaperService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_WALLPAPER [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。
14	Activity (com.ljh.major.module.wallpaper.WallPaperAnimActivity) 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	Broadcast Receiver (com.ljh.major.business.shortcut.PinShortcutCallBackReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
16	Content Provider (com.byted.live.lite.PermissionProvider) 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。
17	Activity (com.blizzard.stepaward.push.OppoPushActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
18	Service (com.blizzard.stepaward.push.service.GTPushService) 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。
19	Broadcast Receiver (com.blizzard.stepaward.push.receiver.RouterBroadcastReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
20	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但是应该检查权限的保护级别。 Permission: com.xiaomi.mipush.permission.MIPUSH_RECEIVE [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。
21	Broadcast Receiver (com.blizzard.stepaward.push.receiver.XMPushMessageReceiver) 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。

22	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 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。
23	Service (com.heytao.msp.push.service.CompatibleDataMessageCallbackService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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。
24	Service (com.heytao.msp.push.service.DataMessageCallbackService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.heytao.mcs.permission.SEND_PUSH_MESSAGE [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。
25	Broadcast Receiver (com.blizzard.stepaward.push.receiver.MeiZuPushMsgReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
26	Service (com.vivo.push.sdk.service.CommandClientService) 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。
27	Broadcast Receiver (com.blizzard.stepaward.push.receiver.VivoPushReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
28	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。
29	Activity 设置了TaskAffinity属性 (com.tool.shortcut.HomeshortcutActivity)	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
30	Activity设置 TaskAffinity属性 (com.tool.shortcut.UninstallFeedbackActivity)	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
31	Activity (com.bytedance.ads.convert.BDBridgeActivity) 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.alipay.sdk.ap p.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。
33	Activity (com.bytedance.an droid.openliveplugin.stub.a ctivity.DouyinAuthorizeActi vityProxy) 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。
34	Activity (com.bytedance.an droid.openliveplugin.stub.a ctivity.DouyinAuthorizeActi vityLiveProcessProxy) 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。
35	Service (com.igexin.sdk.GTI ntentService) 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。
36	Service (com.igexin.sdk.GS ervice) 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。
37	Activity (com.igexin.sdk.Ge tuiActivity) 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。
38	Service (com.meizu.cloud.p ushsdk.NotificationService) 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。
39	Activity (com.xiaomi.mipus h.sdk.NotificationClickedAc tivity) 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。
40	数据短信接收端设置在端口:8 888 上 [android:port]	警告	一个二进制短信接收器被配置为监听一个端口。发送到设备的二进制短信由应用 程序以开发者选择的方式处理。这个短信中的数据应该被应用程序正确地验证。 此外，应用程序应该假设接收到的短信来自一个不可信的来源。

</> 安全漏洞检测

高危: 0 | 警告: 2 | 信息: 1 | 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: MST G-STORAGE-3	升级会员: 解锁高级权限

2	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
3	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

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/libdesdecrypt.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shell code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。	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的搜索路径或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: ['__strlen_chk', '__memcpy_chk', '__vsprintf_chk', '__fgets_chk']	True info 符号被剥离
2	arm64-v8a/libdu.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shell code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的搜索路径或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/libEncryptorP.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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。	Tr u e info 符号被剥离
4	arm64-v8a/libgraphics_tlur.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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。	Tr u e info 符号被剥离

5	arm64-v8a/libluster.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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: ['__strcpy_chk']	Tr u e info 符号被剥离
6	arm64-v8a/libnative-gamesdk.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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。	Tr u e info 符号被剥离

7	arm64-v8a/libsgcore.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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。	Tr u e info 符号被剥离
8	arm64-v8a/libterrain.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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: ['_vsprintf_chk', '_strlen_chk', '_memmove_chk', '_vsprintf_chk']	Tr u e info 符号被剥离

9	arm64-v8a/libxmshell.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shell code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。	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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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: ['__memcpy_chk']	Fa l s e war ni n g 符号可用
10	arm64-v8a/libxysdk-native-lib.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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: ['__vsprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk', '__memset_chk']	Tr u e info 符号被剥离

1 1	arm64-v8a/libxyyoga.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shell code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。	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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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: ['__strlen_chk', '__memcpy_chk', '__vsprintf_chk', '__fgets_chk']	Tr u e info 符号被剥离
1 2	arm64-v8a/libzxprotect.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shell code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。	N o n e info 二进制文件没有设置运行时搜索路径或RPATH。	N o n e 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。	Tr u e 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
00013	读取文件并将其放入流中	文件	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.GET_TASKS android.permission.ACCESS_FINE_LOCATION android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.VIBRATE android.permission.PACKAGE_USAGE_STATS android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	14/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.REORDER_TASKS android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.CHANGE_WIFI_STATE android.permission.BROADCAST_STICKY android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_BACKGROUND_LOCATION com.google.android.gms.permission.AD_ID

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
msg.cmpassport.com	安全	是	IP地址: 124.64.196.20 国家: 中国 地区: 广东 城市: 广州 纬度: 23.127361 经度: 113.264572 查看：高德地图

nisportal.10010.com	安全	是	IP地址: 115.231.163.69 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
id6.me	安全	是	IP地址: 124.64.196.20 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
zxid-m.mobileservice.cn	安全	是	IP地址: 115.231.163.69 国家: 中国 地区: 浙江 城市: 嘉兴 纬度: 30.752199 经度: 120.750000 查看: 高德地图

🌐 URL链接分析

URL信息	源码文件
- https://msg.cmpassport.com/h5/getmobile - https://zxid-m.mobileservice.cn/sdk/said/ping - https://id6.me/gw/preuniq.do - https://nisportal.10010.com:9001	lib/arm64-v8a/libzxprotect.so

📦 第三方SDK

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
Pangle SDK	ByteDance	字节跳动是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
数字联盟可信 ID SDK	北京数字联盟网络科技有限公司	利用数盟可信 ID 技术，可以有效发现行业中各类造假，对于虚拟机造假，数盟可信 ID 不同于 IMEI，MAC，设备序列号，以及 IMSI 等各类设备信息，它不可被篡改，不随 Rom 或者软件的变化而改变。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。

RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
阿里聚安全	Alibaba	阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。

🔑 密钥凭证

可能的密钥
卓信ID-SDK的=> "ZX_APPID_GETUI": "913e6a50-c3b6-4989-8ac6-1ecb53649be3"
vivo推送的=> "com.vivo.push.app_id": "105768915"
vivo推送的=> "com.vivo.push.api_key": "5e06fc3a5ac7ba8f72cac99c1cafb643"
vivo推送的=> "local_iv": "MzMsMzQsMzUsMzYsMzczMzgZmksNDAsNDEsMzlsMzgZmksMzYsMzUsMzQsMzMsMzlsMzQwZWJlLWVudCwzMiwzMiwzMiwzMiwzNCwzMiwzMiwzMiwzMiwzNCw0MSwzNSwzNSwzMiwzMiwzQDMzLDM0LDM1LDM1LDM3LDM4LDM5LDQwLWJlLWVudCwzMiwzMiwzMiwzMiwzLDM0LDMzLDM3LDMzLDM1LDM0LDMzLzCNAMzQsMzlsMzMsMzczMzMsMzQsMzlsMzMsMzMsMzMsMzMsMzQsNDEsMzlsMzlsMzlsMzl"
卓信ID-SDK的=> "ZX_CHANNEL_ID": "C01-GEztJH0JldBC"

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。

© 2025 南明离火 - 移动安全分析平台自动生成