南明离火
移动应用检测平台

ANDROID 静态分析报告

Wyred • v10.29.9.4825

分析日期: 2025-08-25 08:32:29

应用概览

文件名称:	Wyred v10.29.9.4825.apk
文件大小:	21.33MB
应用名称:	Wyred
软件包名:	at.intros.mandiforum
主活动:	com.networkr.ui.launcher.LauncherActivity
版本号:	10.29.9.4825
最小SDK:	28
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	1ecd2e5991c45ff71596cae38f27a91e
SHA1:	909e00ff43042932490020c1600a64798505e4b5d
SHA256:	3f26272662f4b5447cd900fe46a3864f582a7fe27667611f32fe47d9a54d6da4

分析结果严重性分布

高危	中危	信息	安全	关注
2	23	3	3	0

四大组件导出状态统计

Activity组件：15个，其中export的有： 5个
Service组件：13个，其中export的有： 1个
Receiver组件：16个，其中export的有： 7个
Provider组件：4个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: False
v3 签名: True
v4 签名: False
主题: O=GRIP
签名算法: rsassa_pkcs1v15
有效期自: 2019-11-07 15:40:11+00:00
有效期至: 2120-10-13 15:40:11+00:00
发行人: O=GRIP
序列号: 0x2bfe4022
哈希算法: sha256
证书MD5: 12bf82e55af2038e4e0de023ded814c2
证书SHA1: 409e987e1fb369ac73078d8dfc0bcf9fbc91ec43
证书SHA256: 4c6fb675e02453272d5999b178799171b2e67d6f7a80a851f7494bf44f5b38a8
证书SHA512:
8234dad4360309ca3121bbca7ebc1db8f9ffad3b1906ba31e8552c07d1648d5c6d9ab9a3541aba552155ee2c2910a8f6efa613d4881bb32daf9e2075aefe6971

公钥算法: rsa
密钥长度: 2048
指纹: adfd57992f583541c1bc8ae2913c4c06d0651af85101a7d66102bcfb78217450
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.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.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_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.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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。

android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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_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.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。
at.intros.mandiforum.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.RECEIVE_BOOT_COMPLETED	普通	开机启动	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。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。

com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
at.intros.mandiforum.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.networkr.ui.launcher.LauncherActivity	Schemes: networkr://, Hosts: open,

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: **0** | 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: **14** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.networkr.ui.main.MainFragmentActivity) 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。
2	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
3	Activity (com.onesignal.NotificationOpenedActivityHMS) 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。
4	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) 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。
5	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) 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。
6	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) 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。
7	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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 (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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。
9	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。
10	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。
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
12	Activity (androidx.compose.ui.tooling.PreviewActivity) 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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。
14	高优先级 Intent（999）[1 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **1** | 警告: **8** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	应用程序记录日志信息,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	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
3	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
4	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
5	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
6	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
7	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	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
9	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

10	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
11	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
12	已启用远程WebView调试	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
13	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

应用行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	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
00024	Base64解码后写入文件	反射 文件	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
00163	创建新的 Socket 并连接到它	socket	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
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
00091	从广播中检索数据	信息收集	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
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

00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
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
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
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
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
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
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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.VIBRATE android.permission.GET_ACCOUNTS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	11/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_AUDIO com.google.android.c2dm.permission.RECEIVE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
api-prod.grip.events	安全	否	**IP地址:** 52.50.168.114 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
docs.amplify.aws	安全	否	**IP地址:** 18.173.5.15 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
analytics.grip.events	安全	否	**IP地址:** 52.50.168.114 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
docs.aws.amazon.com	安全	否	**IP地址:** 13.33.141.54 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
portal.sso	安全	否	No Geolocation information available.

api2.branch.io	安全	否	**IP地址:** 180.163.150.166 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
events-cdn.grip.events	安全	否	**IP地址:** 13.33.141.54 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
teams-api-prod.grip.events	安全	否	**IP地址:** 52.19.73.112 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
sts.amazonaws.com	安全	否	**IP地址:** 180.163.150.166 **国家:** 美国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.748795 **经度:** -84.387543 **查看:** Google 地图
cdn.branch.io	安全	否	**IP地址:** 13.33.141.102 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
stoplight.io	安全	否	**IP地址:** 104.18.25.178 **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
journeyapps.com	安全	否	**IP地址:** 13.33.141.13 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图

m-and-i.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
www.amazon.com	安全	否	**IP地址:** 13.33.141.13 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
api.onesignal.com	安全	否	**IP地址:** 104.16.160.145 **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
api3-eu.branch.io	安全	否	**IP地址:** 18.173.5.124 **国家:** 丹麦 **地区:** 京畿 **城市:** 哥本哈根 **纬度:** 55.675941 **经度:** 12.565530 **查看:** Google 地图
grip1.typeform.com	安全	否	**IP地址:** 34.235.241.144 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
goo.gle	安全	否	**IP地址:** 104.16.160.145 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图
support.grip.events	安全	否	**IP地址:** 199.60.103.254 **国家:** 美国 **地区:** 马萨诸塞州 **城市:** 剑桥 **纬度:** 42.370129 **经度:** -71.086304 **查看:** Google 地图

firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.162 国家: 中国 地区: 上海 城市: 上海 纬度: 31.230416 经度: 121.473701 查看: 高德地图
portal.sso-fips	安全	否	No Geolocation information available.
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.162 国家: 中国 地区: 上海 城市: 上海 纬度: 31.230416 经度: 121.473701 查看: 高德地图
grip.events	安全	否	**IP地址:** 99.83.190.102 国家: 美国 地区: 华盛顿 城市: 西雅图 纬度: 47.604309 经度: -122.329842 查看: Google地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/aws-amplify/amplify-android/issues	com/amplifyframework/AmplifyException.java
• https://support.grip.events/kb-tickets/new	com/networkr/ui/login/c.java
• https://grip.events/acceptable-use-policy/	Nb/C4645L.java
• https://oidc-fips	q3/a.java
• https://api.onesignal.com/	com/onesignal/core/internal/config/a.java
• http://169.254.169.254	E4/c.java
• https://cognito-identity • https://cognito-identity-fips	R4/C5081c.java
• https://cognito-identity • https://cognito-identity-fips	R4/C1829c.java
• http://169.254.169.254	E4/EnumC3466c.java
• https://storylight.io/mocks/grip/grip-internal-api-documentation:feature%2fps-2017-multiple-sponsor/76618462/ • https://analytics.grip.events/	d3/d.java

• https://stoplight.io/mocks/grip/grip-internal-api-documentation:feature%2fps-2017-multiple-sponsor/76648462/	d3/a.java
• https://github.com/aws-amplify/amplify-android/issues/new	com/amplifyframework/devmenu/DevMenuFileIssueFragment.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	M8/g.java
• https://console.firebase.google.com	I9/AbstractC3924b.java
• https://console.firebase.google.com	I9/AbstractC1574b.java
• https://%s/%s/%s	A9/C2084c.java
• https://grip.events/terms-of-use • https://grip1.typeform.com/to/xcpf6a9w • https://support.grip.events/how-to-scan-badges-and-export-them	la/a.java
• https://plus.google.com/	c7/q0.java
• https://api3-eu.branch.io/ • https://cdn.branch.io/ • https://api2.branch.io/	Fe/v.java
• https://%s/%s/%s	A9/C0559c.java
• www.amazon.com	com/amplifyframework/auth/cognito/helpers/CodegenExtensionsKt.java
• https://docs.amplify.aws/	com/amplifyframework/auth/cognito/helpers/BrowserHelper.java
• https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html	f4/p.java
• http://169.254.170.2	g3/C1341n.java
• https://portal.sso-fips • https://portal.sso	k3/a.java
• http://169.254.170.2	g3/C0566n.java
• https://grip.events/acceptable-use-policy/	Nb/C1153L.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	v6/b.java
• https://sts-fips • https://sts.amazonaws.com	w3/a.java
• https://cognito-idp • https://cognito-idp-fips	x4/C2455c.java
• https://cognito-idp • https://cognito-idp-fips	x4/C6306c.java
• https://goo.gle/compose-feedback	Y0/AbstractC2299p.java
• https://goo.gle/compose-feedback	Y0/AbstractC6453p.java

• https://events-cdn.grip.events/ • https://events-cdn.grip.events/image/	Ya/C6502i.java
• https://events-cdn.grip.events/ • https://events-cdn.grip.events/image/	Ya/i.java
• https://api-prod.grip.events/1/	Ya/n.java
• https://grip.events/privacy-policy/	Yd/c.java
• https://events-cdn.grip.events/ • https://api-prod.grip.events/1/ • https://teams-api-prod.grip.events/1/ • https://analytics.grip.events/ • https://stoplight.io/mocks/grip/grip-internal-api-documentation:feature%2fps-2017-multiple-sponsor/76648462/	z3/C2351c.java
• https://events-cdn.grip.events/ • https://api-prod.grip.events/1/ • https://teams-api-prod.grip.events/1/ • https://analytics.grip.events/ • https://stoplight.io/mocks/grip/grip-internal-api-documentation:feature%2fps-2017-multiple-sponsor/76648462/	z3/C6580c.java
• https://journeyapps.com/ • https://github.com/journeyapps/zxing-android-embedded • https://m-and-i.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://m-and-i.firebaseio.com 的 Firebase 数据库进行通信
Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/717761456800/namespaces/firebase:fetch?key=AIzaSyAIqq0j1WMtv3LzKh16tRJmzwjMIyPgNMw ）已禁用。响应内容如下所示： { "state":"NO_TEMPLATE"

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Compose	Google	Jetpack Compose 是用于构建原生 Android 界面的新工具包。Jetpack Compose 使用更少的代码、强大的工具和直观的 Kotlin API 简化并加快了 Android 上的界面开发。
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。

ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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
info@grip.events support@grip.events	a/a.java

第三方追踪器检测

名称	类别	网址
Amazon Mobile Analytics (Amplify)	Analytics	https://reports.exodus-privacy.eu.org/trackers/423
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

敏感凭证泄露检测

可能的密钥
凭证信息=> "io.branch.sdk.BranchKey" : "@7F13002E"

凭证信息=> "io.branch.sdk.BranchKey.test" : "key_test_cmaRflpm2xyfRC42EZbi9amowrd9yLmo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"branch_key" : "key_live_fiJr9N8WtrVV3m8HxntVafmaAqdT9hSa"
"com.google.firebase.crashlytics.mapping_file_id" : "ab579681e1064c03a8a3dd75194ff862"
"deleteAccountPasswordInputField" : "deleteAccountPasswordInputField"
"firebase_database_url" : "https://m-and-i.firebaseio.com"
"globalSearchSession" : "session"
"globalSearchSessionDate" : "sessionDetailsDateText"
"globalSearchSessionDescription" : "sessionDescription"
"globalSearchSessionLocation" : "sessionDetailsLocationText"
"globalSearchSessionTime" : "sessionDetailsTimeText"
"globalSearchSessionTitle" : "sessionDetailsNameText"
"globalSearchSessionTrack" : "sessionDetailsTrackText"
"google_api_key" : "AIzaSyAIqq0j1WMtv3LzKh16tRJmzwjMIyPgIMw"
"google_app_id" : "1:717761456800:android:237ae998800994cab1b7c5"
"google_crash_reporting_api_key" : "AIzaSyAIqq0j1WMtv3LzKh16tRJmzwjMIyPgIMw"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"loginCreatePasswordButton" : "loginCreatePasswordButton"
"loginCreatePasswordFirstInputField" : "loginCreatePasswordFirstInputField"
"loginCreatePasswordScreen" : "LoginCreatePasswordScreen"
"loginCreatePasswordSecondInputField" : "loginCreatePasswordSecondInputField"
"loginCreatePasswordTitle" : "loginCreatePasswordTitle"
"loginPasswordInputField" : "loginPasswordInputField"
"loginPasswordScreen" : "LoginPasswordScreen"
"nativeListItemUserName" : "nativeListItemUserName"
"passwordLoginButton" : "passwordLoginButton"
"sessionDetailsAddToScheduleButton" : "sessionDetailsAddToScheduleButton"

"sessionDetailsAttendeeListContainer" : "sessionDetailsAttendeeListContainer"

"sessionDetailsContributorsContainer" : "sessionDetailsContributorsContainer"

"sessionDetailsDateIcon" : "sessionDetailsDateIcon"

"sessionDetailsDescriptionContainer" : "sessionDetailsDescriptionContainer"

"sessionDetailsDownloadableContentContainer" : "sessionDetailsDownloadableContentContainer"

"sessionDetailsLocalTimeZone" : "sessionDetailsLocalTimeZone"

"sessionDetailsLocationButton" : "sessionDetailsLocationButton"

"sessionDetailsLocationIcon" : "sessionDetailsLocationIcon"

"sessionDetailsMandatoryAttendanceBadge" : "sessionDetailsMandatoryAttendanceBadge"

"sessionDetailsPlacesLeftContainer" : "sessionDetailsPlacesLeftContainer"

"sessionDetailsPlacesLeftIcon" : "sessionDetailsPlacesLeftIcon"

"sessionDetailsPollingContainer" : "sessionDetailsPollingContainer"

"sessionDetailsPollingIcon" : "sessionDetailsPollingIcon"

"sessionDetailsRemoteTimeZone" : "sessionDetailsRemoteTimeZone"

"sessionDetailsRemoveFromScheduleButton" : "sessionDetailsRemoveFromScheduleButton"

"sessionDetailsScreen" : "SessionDetailsScreen"

"sessionDetailsScrollView" : "sessionDetailsScrollView"

"sessionDetailsSponsorIcon" : "sessionDetailsSponsorIcon"

"sessionDetailsSponsorName" : "sessionDetailsSponsorName"

"sessionDetailsTagsContainer" : "sessionDetailsTagsContainer"

"sessionDetailsTitle" : "sessionDetailsTitle"

"sessionDetailsTrackContainer" : "sessionDetailsTrackContainer"

"sessionDetailsVideoButton" : "sessionDetailsVideoButton"

"sessionDetailsVideoButtonLabel" : "sessionDetailsVideoButtonLabel"

"sessionDetailsWaveSession" : "sessionDetailsWaveSession"

"sessionDetailsWebsiteContainer" : "sessionDetailsWebsiteContainer"

"thingContributorSession" : "session"

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
628ebd3180ca99ac0df2214687966bee
470fa2b4ae81cd56ecbcda9735803434cec591fa
146c5c99-e091-46f9-831c-e60f52fd19b9
8f52694cac5c60bd19ef377904efaeb2
c682b8144a8dd52bc1ad63
515d6767-01b7-49e5-8273-c8d11b0f331d
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

Google Play 应用市场信息

标题: Wyred

评分: None **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** at.intros.mandiforum

开发者信息: Grip - Event Networking Platform, Grip+-+Event+Networking+Platform, None, None, tim@intros.at,

发布日期: 2019年11月20日 **隐私政策:** Privacy link

关于此应用:

Wyred是来自Worldwide Events的突破性的AI驱动的事件应用程序，它将改变您在m&i论坛，TFest，私人豪华事件和Amour上的业务方式！ 该应用程序使用AI对接会技术来帮助您在我们的现场活动中创建面对面的会议，以及全年高质量的虚拟会议。 Netflix使用您的观看历史记录来建议新内容的方式相同，Wyred将分析并识别您的需求以建议未来的业务联系。 有了Wyred，您将永远不会在糟糕的会议上浪费时间。我们的智能技术可确保您仅与满足特定需求的合适人员相匹配。 那你还在等什么？从Worldwide Events下载Wyred事件应用程序，立即开始与您的热门业务匹配关系。

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。