南明离火
移动应用检测平台

ANDROID 静态分析报告

GBM

GBM • v1.3.0

分析日期: 2025-04-05 08:33:02

应用概览

文件名称:	GBM v1.3.0.apk
文件大小:	39.93MB
应用名称:	GBM
软件包名:	com.gbm.app
主活动:	com.gbm.linking.presentation.component.LinkingActivity
版本号:	1.3.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	7/432
杀软检测:	经检测，该文件安全
MD5:	cb914d0b1c08ac1eff39ff1dbfc8d467
SHA1:	d9074775f989d994519fa6de26a8cf915ba5123e
SHA256:	51682d2195e7d7453e07a6e0338ed53caf39439da4eb253aee4ebabb64656a

分析结果严重性分布

高危	中危	信息	安全	关注
3	27	2	4	1

四大组件导出状态统计

Activity组件：61个，其中export的有： 12个
Service组件：21个，其中export的有： 1个
Receiver组件：20个，其中export的有： 3个
Provider组件：7个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-28 23:11:18+00:00
有效期至: 2053-08-28 23:11:18+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x35f18d5311a8e7665daae5f35644a5fab4f13b14
哈希算法: sha256
证书MD5: effd2462921751e971010dcd12b80014
证书SHA1: 3336930872d63ebc38089b87b203b55767ff002e
证书SHA256: 27466dd03a28998cea48976e1b2ce57c8901e005276797edd4b3e9ce63775490
证书SHA512:
b14b07feb880c351ac5d5de7bd26ae3f54e995f055caa8b615b2129299a2d183038b5e3ebf6f0ca63ee85bdf362e2e8b9[illegible]c8e193d5870aeb2083a4f4a2d90

公钥算法: rsa
密钥长度: 4096
指纹: 1882bb208295fa3d527ffa2e6fe2c0474c6348f53c56393d7da7c3db85b61463
找到 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_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。
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.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.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.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.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。
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.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.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.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.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.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。
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。
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。
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进行启动。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.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。
com.gbm.app.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.gbm.linking.presentation.component.LinkingActivity	Schemes: https://, Hosts: gbm.page.link, gbm.jre.agconnect.link, auth.gbm.com, Path Patterns: /confirmation, /password-recovery,
com.useinsider.insider.InsiderLoginActivity	Schemes: insidergbm2://,

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	Activity (androidx.compose.ui.tooling.PreviewActivity) 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。
2	Activity (com.walmartlabs.ern.container.miniapps.AnalyticsBridgeMiniappActivity) 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。
3	Activity (com.walmartlabs.ern.container.miniapps.AnnouncementsMiniappActivity) 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。
4	Activity (com.walmartlabs.ern.container.miniapps.DayTradesMiniappActivity) 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.walmartlabs.ern.container.miniapps.DepositsMiniappActivity) 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	Activity (com.walmartlabs.ern.container.miniapps.HelpMiniappActivity) 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。
7	Activity (com.walmartlabs.ern.container.miniapps.LoginHistoryMiniappActivity) 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。
8	Activity (com.walmartlabs.ern.container.miniapps.SmartCashDashboardMiniappActivity) 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。
9	Activity (com.walmartlabs.ern.container.miniapps.TradingOperationMiniappActivity) 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。
10	Activity (com.walmartlabs.ern.container.miniapps.TransferFlowMiniappActivity) 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。
11	Activity (com.walmartlabs.ern.container.miniapps.WelcomeMiniappActivity) 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。

12	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver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。
13	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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。
15	Activity (com.useinsider.insider.InsiderLoginActivity) 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。
16	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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。

代码安全漏洞检测

高危: **2** | 警告: **10** | 信息: **2** | 安全: **3** | 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	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
3	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

4	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
5	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
6	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
7	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
8	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
9	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	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-2	升级会员：解锁高级权限
10	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
11	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

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	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
14	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
15	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
16	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
17	此应用程序使用Safety Net API。	安全	OWASP MASVS: MSTG-RESILIENCE-7	升级会员：解锁高级权限

应用行为分析

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
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
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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00080	将录制的音频/视频保存到文件	录制音视频 文件	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	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

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
00136	停止录音	录制音视频 命令	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
00090	设置录制的音频/视频文件格式	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
00138	设置音频源（MIC）	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
00133	开始录音	录制音视频 命令	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
00024	Base64解码后写入文件	反射 文件	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
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
00147	获取当前位置的时间	信息收集 位置	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
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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
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
00192	获取短信收件箱中的消息	短信	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
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00185	开始将相机预览帧捕获到屏幕上	相机	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
00009	将游标中的数据放入JSON对象	文件	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
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
00092	发送广播	命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	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
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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00182	打开相机	相机	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	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
00132	查询ISO国家代码	设备信息 信息收集	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00041	将录制的音频/视频保存到文件	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
00130	获取当前WIFI信息	WiFi 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	7/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.VIBRATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	10/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE

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
conf.rollout.io	安全	否	**IP地址:** 54.84.159.236 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
origin.app.stg-gbm.com	安全	否	**IP地址:** 54.84.159.236 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
qa-statestore.rollout.io	安全	否	**IP地址:** 3.169.183.113 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
gbm.com	安全	否	**IP地址:** 104.236.203.177 **国家:** 美国 **地区:** 新泽西州 **城市:** 克利夫顿 **纬度:** 40.858585 **经度:** -74.163605 **查看:** Google 地图

development-statestore.rollout.io	安全	否	**IP地址:** 108.138.246.86 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
qa-api.rollout.io	安全	否	**IP地址:** 34.195.159.22 **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
qaanalytic.rollout.io	安全	否	**IP地址:** 3.213.136.68 **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
pinterest.com	安全	否	**IP地址:** 54.175.250.85 **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
auth.gbm.com	安全	否	**IP地址:** 172.66.0.227 **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
push.rollout.io	安全	否	**IP地址:** 54.204.28.160 **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
twitter.com	安全	否	**IP地址:** 172.66.0.227 **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
mobileanalytics.tiktok.com	安全	否	No Geolocation information available.

notify.bugsnag.com	安全	否	**IP地址:** 35.186.205.6 **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
statestore.rollout.io	安全	否	**IP地址:** 18.239.199.63 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
qax-push.rollout.io	安全	否	**IP地址:** 54.84.159.236 **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
mobile.useinsider.com	安全	否	**IP地址:** 18.239.199.63 **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
analytic.rollout.io	安全	否	**IP地址:** 54.84.159.236 **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
qa-conf.rollout.io	安全	否	**IP地址:** 3.169.183.47 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
api.appgbm.com	安全	否	**IP地址:** 159.60.143.252 **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
gbmprojects.atlassian.net	安全	否	**IP地址:** 104.192.140.20 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图

development-conf.rollout.io	安全	否	**IP地址:** 18.244.214.5 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
api.omni.gbmapi.com	安全	否	**IP地址:** 18.238.192.66 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
dbv3au4xbiamq.cloudfront.net	安全	否	**IP地址:** 65.8.161.80 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
x-api.rollout.io	安全	否	**IP地址:** 50.17.237.115 **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
assets.gbm.com	安全	否	**IP地址:** 165.22.235.237 **国家:** 加拿大 **地区:** 安大略 **城市:** 多伦多 **纬度:** 43.653660 **经度:** -79.382927 **查看:** Google 地图
api.mixpanel.com	安全	否	**IP地址:** 107.178.240.159 **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.gbmfondos.com.mx	安全	否	**IP地址:** 3.169.183.112 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
appgallery.huawei.com	安全	是	**IP地址:** 49.4.34.28 **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.smpte-ra.org	安全	否	**IP地址:** 52.20.185.129 **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
• http://www.unicode.org/terms_of_use.html • http://www.unicode.org/reports/tr24/ • http://sourceforge.net/adobe/aglfn/ • http://www.unicode.org/reports/tr44/ • http://www.unicode.org/unicode/reports/tr9/	自研引擎-A
• https://api.appgbm.com	com/gbm/buying/power/di/BuyingPowerDataModuleKt.java
• https://auth.gbm.com/api/ • https://api.appgbm.com	com/gbm/patron/data/di/features/SourcesDataModuleKt.java
• https://www.gbmfondos.com.mx/files/pdf/soluciones/fisicas/prospectos/prospecto_%1$s.pdf • https://assets.gbm.com/trading/fact-sheets/%1$s.pdf	com/gbm/instrument/presentation/BuildConfig.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramStoriesShare.java
• https://api.appgbm.com	com/gbm/instrument/di/SecurityDetailDataModuleKt.java
• https://api.mixpanel.com	com/mixpanel/android/util/MPConstants.java
• https://auth.gbm.com/	com/gbm/patron/data/BuildConfig.java
• https://api.appgbm.com	com/gbm/web/snacks/legal/data/di/features/LegalDocumentDataModuleKt.java
• https://api.appgbm.com	com/gbm/watchlist/data/di/WatchlistDataModuleKt.java
• https://api.appgbm.com	com/gbm/common/data/di/features/SourceDataModuleKt.java
• https://api.appgbm.com	com/gbm/order/di/OrderDataModuleKt.java
• https://api.appgbm.com	com/gbm/market/common/di/SourcesDataModuleKt.java
• https://play.google.com/store/apps/details?id=	com/medallia/digital/mobilesdk/e3.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java

• https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
• https://dbv3au4xbiamq.cloudfront.net?type=database&pageid=5ae80d98a14a4bcbaf76b191ee83cbdf&subroutes=1&webview=true&analytics=wealth	com/gbm/wealth/presentation/navigation/ComposableSingletons$GoalDetailNavGraphKt.java
• https://auth.gbm.com/	com/gbm/mfa/data/BuildConfig.java
• https://api.appgbm.com	com/gbm/position/di/PositionDataModuleKt.java
• https://api.appgbm.com	com/gbm/instrument/finder/di/InstrumentFinderDataModuleKt.java
• https://api.appgbm.com	com/gbm/my/instruments/di/MyInstrumentDataModuleKt.java
• https://api.appgbm.com	com/gbm/movement/data/BuildConfig.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
• https://api.appgbm.com	com/gbm/movement/data/di/features/SourceDataModuleKt.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramShare.java
• https://qa-conf.rollout.io • http://10.0.2.2:8887/sse • https://qa-api.rollout.io • https://analytic.rollout.io • https://push.rollout.io/sse • http://10.0.2.2:8557 • https://conf.rollout.io • http://127.0.0.1:8787 • https://x-api.rollout.io • https://qaanalytic.rollout.io • https://development-conf.rollout.io • https://qax-push.rollout.io/sse • http://127.0.0.1:8557 • https://development-statestore.rollout.io • https://qa-statestore.rollout.io • http://10.0.2.2:8787 • http://127.0.0.1:8887/sse • https://statestore.rollout.io	io/rollout/client/Environment.java
• https://api.appgbm.com	com/gbm/wealth/data/di/features/SourceDataModuleKt.java
• https://www.google.com	com/rizzi/bouquet/network/RetrofitProviderKt.java
• https://dbv3au4xbiamq.cloudfront.net • https://api.appgbm.com • https://api.appgbm.com/	com/gbm/common/data/BuildConfig.java
• https://auth.gbm.com/api/	com/gbm/mfa/data/di/features/SourcesDataModuleKt.java

本报告由南明离火移动安全分析平台生成

• https://notify.bugsnag.com	io/rollout/reporting/ErrorReporter.java
• file:file	com/huawei/location/lite/common/log/logwrite/LogWrite.java
• http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	org/mp4parser/muxer/tracks/ttml/TtmlHelpers.java
• https://api.appgbm.com	com/gbm/upgrade/data/di/features/SourcesDataModuleKt.java
• http://%s/bundles/%s/android • http://%s/stores	com/walmartlabs/ern/container/devassist/ErnDevSettingsActivity.java
• https://api.omni.gbmapi.com/	com/gbm/upgrade/data/BuildConfig.java
• https://github.com/mixpanel/mixpanel-android/issues/567	com/mixpanel/android/mpmetrics/AnalyticsMessages.java
• https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.java
• https://api.appgbm.com	com/gbm/web/snacks/legal/data/BuildConfig.java
• https://assets.gbm.com/wm/fact-sheets/latest/1_liquidezf.pdf • https://assets.gbm.com/wm/fact-sheets/latest/5_apreciacionf.pdf • https://gbm.com/academy/ • https://origin.app.stg-gbm.com/docs/marco_general_de_actuacion_v3.pdf • https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2 • https://mobile.useinsider.com/api/v1/geofences • https://assets.gbm.com/wm/fact-sheets/latest/6_crecimientof.pdf • https://mobile.useinsider.com/api/logging/sdk/v2 • https://mobile.useinsider.com/api/v1/geofences/notify • https://github.com/vinc3m1/roundedimageview • https://gbmprojects.atlassian.net/wiki/spaces/technology/pages/2899804173/event+naming+conventions+%7c+ae • https://play.google.com/store/apps/details?id=%1 • https://mobile.useinsider.com/api/gandalf/v2/start_connection • https://github.com/vinc3m1 • https://mobile.useinsider.com/api/v2/assurance/set • https://mobile.useinsider.com/api/v1/privacy/gdpr/consent/get • https://play.google.com/store/apps/details?id=com.authy.authy • https://assets.gbm.com/wm/fact-sheets/latest/7_bolsaf.pdf • https://appgallery.huawei.com/#/app/c109279503 • https://auth.gbm.com/docs/jurisdiccion-aplicable.pdf • https://mobile.useinsider.com/api/v3/session/stop • https://mobile.useinsider.com/api/v1/privacy/gdpr/consent/set • https://assets.gbm.com/wm/fact-sheets/latest/2_deudaf.pdf • https://play.google.com/store/apps/details?id=com.azure.authenticator • https://mobileanalytics.useinsider.com • https://mobile.useinsider.com/api/v1/test_device/add • https://mobile.useinsider.com/api/v1/message_center/get • https://mobile.useinsider.com/api/identity/v1/get • https://mobile.useinsider.com/api/v2/social/view • https://mobile.useinsider.com/api/v3/session/start • https://mobile.useinsider.com/api/amplification/v1/poll • https://mobile.useinsider.com/api/gandalf/v2/live_push • https://mobile.useinsider.com/api/gandalf/v2/stop_connection • https://assets.gbm.com/wm/fact-sheets/latest/4_balancef.pdf • https://auth.gbm.com/docs/aviso-de-privacidad.pdf • https://assets.gbm.com/wm/fact-sheets/latest/3_preservacionf.pdf • https://github.com/vinc3m1/roundedimageview.git	自研引擎-S

本报告由南明离火移动安全分析平台生成

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/850485699609/namespaces/firebase:fetch?key=AIzaSyCyH6TTyFtOZ-QsEgVTgb-Px_-7ak70CSU ） 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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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

plus@gbm.com	com/gbm/common/presentation/utils/EmailUtils.java
no-reply@gbm.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Insider	Analytics	https://reports.exodus-privacy.eu.org/trackers/409
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

敏感凭证泄露检测

可能的密钥
凭证信息=> "rox.apiKey" : "@string/rollout_key"
"auth_app_link_authy" : "https://play.google.com/store/apps/details?id=com.authy.authy"
"auth_app_package_authy" : "com.authy.authy"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"default_password_one" : "Password"
"facebook_app_id" : "2959991933576[illegible]"
"facebook_client_token" : "023a[illegible]7cbe00b36ee30740c[illegible]080bb43b2"
"google_api_key" : "AIzaSyCyH6TTyFtOZ-QsEgVTgb-Px_-7ak70CSU"
"google_app_id" : "1:850485699609:android:d9[illegible]eec6e810b582ab688"
"google_crash_reporting_api_key" : "AIzaSyCyH6TTyFtOZ-QsEgVTgb-Px_-7ak70CSU"
"help_center_key" : "help_center_key"
"insider_session_custom_start" : "/api/v3/session/start"
"insider_session_custom_stop" : "/api/v3/session/stop"
"insider_session_start" : "https://mobile.useinsider.com/api/v3/session/start"
"insider_session_stop" : "https://mobile.useinsider.com/api/v3/session/stop"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"password_dialog_tag" : "Seguridad"
"rollout_key" : "63d97308d57a448237646bd1"
"tax_documents_cache_key" : "tax_documents"
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
XK3VwBIDCibTJtek6TaafiDAXvAdVURWIPy
eyJzdWIiOiJhcGlUb2tlblYyIiwiYXV0aFVybCI6Imh0dHBzOi8vZ2JtLm1kLWFwaXMubWVkYWxsaWEuY29tL21vYmlsZVNESy92MS9hY2NlcHQtb2tlbiIsImVudmlyb25tZW50IjoiZGlnaXRhbC1jbG91ZC13ZXN0IiwiY3JlYXRlVGltZSI6MTYzNTE3Mzg5Mjg0NSwiZG9tYWluIjoiaHR0cHM6Ly9nYm0ubWVQfYXBpLy5tZWRhbGxpYS5jb20vIiwiYXBpVG9rZW5WMlZlcnNpb24iOjIsInByb3BlcnR5SWQiOjE0NTc2Mn0
af00ffe52e8f71422165ad54f34ecd76
239CA10A1AFB3998BF91FA08A9F8C2FE73CB4A171703F7206AE5702A5F07E011
0924b35e-fc4e-47f9-a629-7fbcb8e633d9
ntTEswySdSdPz3KpuEeHIPhQp3vkANNeSCYemFOLrfZv5EJd7
9A04F079-9840-4286-AB92-E65BE0885F95
61fd762924b05d0019cfa8db
eec93abb416cd00d3db6b932b7a9710e
a67422af-8504-43df-9e63-7361eb0bd99e
3370fec94530814e4810fcb12b44c599
bbfe67a2-8481-4870-8853-7b5c7b9253cc
64ef690ea08946719761292b0aff928f
506d5ae2-a45b-498d-927d-12ac041d2591
4eb3138f4e59640e948b9c91a1929e13
df6b721c8b4d3b6eb44c861d4415007a5a35fc95
cc7c78e948089ced4a753e91ca9543f8
9b8f518b086098de3d77736f9458a3d2f6f95a37
2438bce1ddb7cd026d5ff89f598b3b5e5bb824f3
sha256/cGJuAXyFXFkWm61cF4HPWX8S0XS9j0aSqN0k4AP+4A=
A2B55680-6F43-11E0-9A3F-0002A5D5C51B
sGiv1GlNwVeTSjoglqDSNdc3CZibn7DkgMY62tRtcF8u7VX43YYFACUc4RWp4VFFFT
QzIhw4ewzpr5TCsH2AE70Kx0As8Z
85053bf7[illegible]75239b16a601d9387e17
c56fb7d591ba6704df047fd98f535372fea00211
sha256/DXHPcgpOWkA82Sz+q6rbZuNq9TH4GMRmEEeeEETV+90=

本报告由南明离火移动安全分析平台生成

bbcc38c74221f40e7d4d2438dab7c61d
cc2751449a350f668590264ed76692694a80308a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
b744e88bf5b1a800e3155af233dbdc51
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
9608869e-3d13-4b1d-b252-f38ca6b81ea1
61fd7739c617f40013487c16
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
8iYhOFfkoA3cVZj2Pl51N21v7xvJDYG8TnPPhxdtMHWBj3e6hXDnclbhs
5ae80d98a14a4bcbaf76b191ee83cbdf
ddba241c-7fe1-413b-b52f-7cffafa95631
97e7e70f4c0c4b4996d53b1de51b96cc
40af6442001c6a6bd610721bfbbcba87
201c9f7c5a3a4b3741239bcf64d9df78

Google Play 应用市场信息

标题: GBM

评分: 3.8070796 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.gbm.app

开发者信息: GBM.COM, GBM.COM, None, https://gbm.com/, plus@gbm.com,

发布日期: 2023年10月16日 **隐私政策:** Privacy link

关于此应用:

欢迎使用 GBM 应用程序！ 将您的所有投资集中在一处。查看市场走势和您的金融工具的详细信息。随时随地以便捷的方式进行投资。 您可以使用 GBM 应用程序做什么？ 智能现金 从储蓄转向投资，无需费用或佣金即可获得每日回报。通过投资政府工具，让您的资金安全增长。此外，您还可以在工作日上午 7:30 至下午 1:00 轻松存取资金。 智能现金元 通过以方便且简单的方式投资美元，使您的投资组合多样化。您将能够通过以美元计价的债务工具利用美元的强势和稳定性。此外，您可以随时存款，工作日提款，结算时间为24个工作日。 市场 买卖各种工具，如 ETF、固定收益债务基金以及国家和美国股票。获得工具后，您将能够从交易部分查看它们。 目标 借助 Asesoría+，您可以自定义您的投资组合，以适应并设定您想要的所有目标。我们了解您的目标，并为您提供数字建议和投资策略，以实现您的目标。长期投资从未如此容易 你有疑问吗？ 我们有一个包含常见问题的部分，以便您可以回答所有问题。 我们不断发展，为您提供越来越多的功能！ GBM，墨西哥投资的地方。 更多信息请访问 gbm.com 。 Av. Insurgentes Sur No. 1605, San José Insurgentes, Benito Juárez 03900 墨西哥城, 墨西哥

免责声明及风险提示: