南明离火
移动应用检测平台

# ANDROID 静态分析报告

Bugko • v9.2.6.0



分析日期: 2025-08-29 15:32:33

# 应用概览

| | |
|---|---|
| 文件名称: | Bugko v9.2.6.0.apk |
| 文件大小: | 30.12MB |
| 应用名称: | Bugko |
| 软件包名: | com.bugko |
| 主活动: | crc6455d3dd4cdc9e7ca2.SplashActivity |
| 版本号: | 9.2.6.0 |
| 最小SDK: | 21 |
| 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: | 57/100 (中风险) |
| 跟踪器检测: | 4/432 |
| 杀软检测: | 经检测，该文件安全 |
| MD5: | bd0072f36710f4d46fb8379a40ec79d0 |
| SHA1: | af181e8d27066c[illegible]9b37bb9ef3f6fbe[illegible]5a2 |
| SHA256: | 9307966b[illegible]7c3a73a3507b701c[illegible]200ba92baf5db50b03170015ede94 |



## 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 0 | 16 | 2 | 2 | 0 |

## 四大组件导出状态统计

| |
|---|
| Activity组件：85个，其中export的有： 2个 |
| Service组件：14个，其中export的有： 2个 |
| Receiver组件：18个，其中export的有： 3个 |

Provider组件：8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=60
签名算法: rsassa_pkcs1v15
有效期自: 2016-11-01 06:24:07+00:00
有效期至: 2046-10-25 06:24:07+00:00
发行人: C=60
序列号: 0x3817ced4
哈希算法: sha256
证书MD5: af7a3e2f6d58c8195ae071cd4523d7f8
证书SHA1: 479bad4d912742ed7cf887ed81349ffa5b8c32d0
证书SHA256: 8de22424b943119c857fd8578185d4dff07923f91e203c151bf0f2cf5d78d616
证书SHA512:
e91071f488d1e29f1d19e2154c46f78327135f8304bf016c7170542a1f71a9545abbd500d79f22343...100f15bf3a6e6524494b...f85172c77c9bb1921ba7ba

公钥算法: rsa
密钥长度: 2048
指纹: 3fea5d80149d0dc796e9b9de97f2337f2c429ce4732eae4bd1c2a74bdfab07f...
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.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.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.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.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.VIBRATE | 普通 | 控制振动器 | 允许应用程序控制振动器，用于消息通知振动功能。 |
| android.permission.CAMERA | 危险 | 拍照和录制视频 | 允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。 |
| com.bugko.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | 未知权限 | 来自 android 引用的未知权限。 |

| | | | |
|---|---|---|---|
| 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.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.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.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_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。 |
| 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_TOPICS | 普通 | 允许应用程序访问广告服务主题 | 这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。 |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | 普通 | 由 Google 定义的权限 | 由 Google 定义的自定义权限。 |

## 可浏览 Activity 组件分析

| ACTIVITY | INTENT |
|---|---|
| crc6455d3dd4cdc9e7ca2.DropboxCallbackActivity | Schemes: com.bugko.dropbox://,<br>Paths: /oauth2redirect, |

## 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: **9** | 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 | 应用数据允许备份 [android:allowBackup=true] | 警告 | 该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。 |
| 3 | 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。 |
| 4 | Service (crc640190106674015c54.PushNotificationMessagingService) 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。 |
| 5 | Activity (crc6455d3dd4cdc9e7ca2.DropboxCallbackActivity) 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 (crc6455d3dd4cdc9e7ca2.InitializeActivity) 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 | BroadcastReceiver (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。 |

| | | | |
|---|---|---|---|
| 8 | Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.BIND_JOB_SERVICE<br>[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。 |
| 9 | Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.DUMP<br>[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。 |

## 代码安全漏洞检测

高危: **0** | 警告: **5** | 信息: **1** | 安全: **1** | 屏蔽: **0**

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|---|---|---|---|---|
| 1 | IP地址泄露 | 警告 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2 | 升级会员：解锁高级权限 |
| 2 | 应用程序记录日志信息,不得记录敏感信息 | 警告 | CWE: CWE-532: 通过日志文件的信息暴露<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |
| 3 | SHA-1是已知存在哈希冲突的弱哈希 | 警告 | CWE: CWE-327: 使用一破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 4 | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 5 | 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 |

| | | | | |
|---|---|---|---|---|
| 6 | 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<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | 升级会员：解锁高级权限 |
| 7 | 此应用程序可能会请求root（超级用户）权限 | 警告 | CWE: CWE-250: 以不必要的权限执行<br>OWASP MASVS: MSTG-RESILIENCE-1 | 升级会员：解锁高级权限 |

## 应用行为分析

| 编号 | 行为 | 标签 | 文件 |
|---|---|---|---|
| 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 |
| 00012 | 读取数据并放入缓冲流 | 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<br>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<br>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<br>命令 | 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 | 4/30 | android.permission.VIBRATE<br>android.permission.CAMERA<br>android.permission.WAKE_LOCK<br>android.permission.RECEIVE_BOOT_COMPLETED |
| 其它常用权限 | 9/46 | android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.FOREGROUND_SERVICE<br>com.google.android.c2dm.permission.RECEIVE<br>com.google.android.gms.permission.AD_ID<br>com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE |

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

## 恶意域名威胁检测

| 域名 | 状态 | 中国境内 | 位置信息 |
| --- | --- | --- | --- |
| bugko-com.firebaseio.com | 安全 | 否 | **IP地址:** 34.120.206.254<br>**国家:** 美国<br>**地区:** 密苏里州<br>**城市:** 堪萨斯城<br>**纬度:** 39.099731<br>**经度:** -94.578568<br>**查看:** Google 地图 |

## URL 链接安全分析

| URL信息 | 源码文件 |
| --- | --- |
| • http://10.0.2.2:8969/stream | io/sentry/SpotlightIntegration.java |
| • https://bugko-com.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://bugko-com.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/676853876661/namespaces/firebase:fetch?key=AIzaSyC_3or491Z50TnyQAJvotKOGAdcNzdJaM8 ）已禁用。响应内容如下所示：<br>{<br>"state": "NO_TEMPLATE"<br>} |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
| --- | --- | --- |
| 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。 |
| 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。 |


本报告由南明离火移动安全分析平台生成

| | | |
|---|---|---|
| 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 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 |
|---|---|
| help@bugko.com | 自研引擎-S |

## 第三方追踪器检测

| 名称 | 类别 | 网址 |
|---|---|---|
| Google AdMob | Advertisement | https://reports.exodus-privacy.eu.org/trackers/312 |
| Google CrashLytics | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/27 |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |
| Sentry | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/447 |

## 敏感凭证泄露检测

| 可能的密钥 |
|---|
| AdMob广告平台的key "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-0646444153861496~6958753653" |
| "firebase_database_url" : "https://bugko-com.firebaseio.com" |
| "google_api_key" : "AIzaSyC_3or491Z50TnyQAJvotKOGAdcNzdJaM8" |
| "google_app_id" : "1:676853876661:android:d15840cb41d4a8d4" |


本报告由南明离火移动安全分析平台生成

"google_crash_reporting_api_key" : "AIzaSyC_3or491Z50TnyQAJvotKOGAdcNzdJaM8"

# Google Play 应用市场信息

**标题:** Bugko - MTG Companion App

**评分:** 4.65 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.bugko

**开发者信息:** ooikengsiang, ooikengsiang, None, http://bugko.com, help@bugko.com,

**发布日期:** 2016年10月31日 **隐私政策:** Privacy link

**关于此应用:**

Bugko是一款专为Magic：The Gathering（MTG）玩家和法官设计的非官方应用程序（由粉丝制作）多合一伴侣应用程序。 Bugko专注于提供独特的核心功能，例如新闻汇总，剧透警报，锦标赛卡组列表更新，卡语法搜索等等。 Bugko还内置了其他熟悉的功能，例如生命计数器，愿望清单，收集跟踪器，离线卡搜索，随机卡，综合规则，甲板构建，以提供完整的体验。 Bugko将是您真正喜欢的第一个现代设计的MTG应用程序。 Bugko是唯一将所有喜爱的MTG，MTGO和Arena新闻来源整合到一起的应用程序。目前可用的新闻频道包括Fireball频道，MTGS频道，Mythic Spoiler，Star City Games和40多个新闻来源。打开应用程序后，您可以滚动浏览当前发生的所有新闻和剧透。借助应用程序中的推送通知，您一定不会错过自己喜欢的新闻频道中的任何重要新闻更新。最新的宠坏卡？布格让你受够了。 Bugko具有强大而又可脱机访问的卡数据库。您可以选择使用专为高级用户设计的超快速语法搜索来搜索30,000+张卡片，也可以仅使用用户友好界面提供的搜索过滤器。借助直接从TCGPlayer和Cardmarket获得的最新卡价格，您可以随时随地查看，购买，交易或跟踪您的收藏。 您是魔术师吗？ Bugko具有专门为法官设计的工具，脚本脚本计时器，《违规程序指南》（IPG）参考，《魔术比赛规则》（MTR）文档，具有完整搜索功能的离线综合规则等。Bugko中的许多功能均经过精心设计，可满足法官的需求。例如，离线卡数据库，多种语言的卡文本，判断博客或新闻更新等等。非常适合周游世界的法官。 特征： -来自40多个热门新闻频道的最新MTG新闻和剧透，带有通知警报。 -生命计数器支持2-8位玩家，15个不同的计数器，计数器更改历史记录，法力池和现代设计。 -离线完整的数据库，包括所有最新印刷的卡，促销卡，11种以上印刷语言，20种以上格式的黑名单，卡片裁定，保留列表等。 -强大的卡片搜索引擎，支持语法搜索，25种以上的卡片属性过滤器，随机卡片等。 -最新的卡定价，包括所有促销卡，铝箔卡，直接来自TCGPlayer或Cardmarket的各种艺术品。 -提供30多种货币的自动货币转换器。 -随时随地以最新价格跟踪您的收款，交易和愿望清单。 -甲板制造商，赢得标准，现代和传统格式的甲板奖。 -法官的工具，例如离线可搜索的综合规则，MTG，IPG，快速参考，脚本草稿计时器，甲板清单计数器，离线文档等。 免责声明：Magic：The Gathering（也称为MTG）卡设计，文本，图像，扩展和符号是Hasbro，LLC的Wizards of the Coast的商标和版权。 Bugko与Wizards of the Coast LLC不隶属，不认可，不赞助或未特别批准。

---

## 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。