南明离火
移动应用检测平台

# ANDROID 静态分析报告


蜜臀 • v1.6.9

分析日期: 2024-03-19 16:36:04

# 应用概览

| | |
|---|---|
| 文件名称: | MIM18QS3.apk |
| 文件大小: | 21.58MB |
| 应用名称: | 蜜臀 |
| 软件包名: | com.tmmomooba.gsjefxbbjzdezfztvdazagyrzqiutydrwboea |
| 主活动: | com.limit.cache.ui.page.main.WelComeActivity |
| 版本号: | 1.6.9 |
| 最小SDK: | 21 |
| 目标SDK: | 34 |
| 加固信息: | 未加壳 |
| 应用程序安全分数: | 61/100 (低风险) |
| 杀软检测: | AI评估：可能有安全隐患 |
| MD5: | 20e17866ff2ba7ab8d22334088054104 |
| SHA1: | cd4ab78b64104b288612201e08f885eebfa32e659 |
| SHA256: | 744163d3a1e1729d7d236e3a7a57afaa6501805511be33050413c43326316ab |

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 0 | 5 | 10 | 1 | 0 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：80个，其中export的有：0个 |
| Service组件：7个，其中export的有：0个 |
| Receiver组件：4个，其中export的有：1个 |
| Provider组件：6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: False
v2 签名: False
v3 签名: False


本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: ST=(湖南), L=(湖南), O=(枷汁畜铃暮普罢脸参哺), OU=(铝颈狼篡补豢泼休), CN=(挑话瓜祷吕)
签名算法: dsa
有效期自: 2024-03-18 12:01:05+00:00
有效期至: 2124-02-23 12:01:05+00:00
发行人: ST=(湖南), L=(湖南), O=(枷汁畜铃暮普罢脸参哺), OU=(铝颈狼篡补豢泼休), CN=(挑话瓜祷吕)
序列号: 0x5d1618ce
哈希算法: sha256
证书MD5: daf71e4e44af157db56180aa2a0b5160
证书SHA1: 83a75535ac3b77632fc56bc305f4788578537e38
证书SHA256: 75f212da98970962d2e22a3b03b64743a4007a9354bd08ed61d673de6de3523a
证书SHA512:
15d76673b45765dde8b48a0271e5ad6939fd3dfbe0bbcb8bfe94cf2a22f94be66b2df7b68fa99192c5514ea2c776b532af0c559e075e9d43c[illegible]34a41b42cd4

公钥算法: dsa
密钥长度: 1024
指纹: e30fe02be208df5d7ca8c88aa52f5a5095103f1acb830371fc82bb069ab2192a
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_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错略的经纬度信息，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.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_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.READ_PRIVILEGED_PHONE_STATE | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| 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。 |
| 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_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.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.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.REQUEST_DELETE_PACKAGES | 普通 | 请求删除应用 | 允许应用程序请求删除包。 |

| | | | |
|---|---|---|---|
| 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_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.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.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.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.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（播放悬浮播放，锁屏播放） |
| com.tmmomooba.gsjefxbbjzdezfztvdazagyrzqiutydrwboea.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 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。 |
| 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.FLASHLIGHT | 普通 | 控制闪光灯 | 允许应用程序控制闪光灯。 |

## 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 | 应用程序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: **4** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
|---|---|---|---|
| 1 | 应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2 [minSdk=21] | 警告 | 该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。 |
| 2 | 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。 |

| | | | |
|---|---|---|---|
| 3 | 应用程序具有网络安全配置 [android:networkSecurityConfig=@null] | 信息 | 网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。 |
| 4 | 应用程序数据可以被备份 [android:allowBackup=true] | 警告 | 这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。 |
| 5 | 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

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|---|---|---|---|---|

## 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/librtmp-jni.so | True<br>info<br>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。 | True<br>info<br>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 | True<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或RPATH | None<br>info<br>二进制文件没有设置RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__strrchr_chk', '__vsnprintf_chk', '__memcpy_chk', '__strchr_chk', '__vsprintf_chk', '__strncpy_chk'] | False<br>warning<br>符号可用 |

## 敏感权限滥用分析

| 类型 | 匹配 | 权限 |
| --- | --- | --- |
| 恶意软件常用权限 | 8/30 | android.permission.ACCESS_COARSE_LOCATION<br>android.permission.ACCESS_FINE_LOCATION<br>android.permission.READ_PHONE_STATE<br>android.permission.VIBRATE<br>android.permission.GET_TASKS<br>android.permission.CAMERA<br>android.permission.CALL_PHONE<br>android.permission.REQUEST_INSTALL_PACKAGES |
| 其它常用权限 | 12/46 | android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.READ_MEDIA_IMAGES<br>android.permission.READ_MEDIA_AUDIO<br>android.permission.READ_MEDIA_VIDEO<br>android.permission.CHANGE_WIFI_STATE<br>android.permission.FOREGROUND_SERVICE<br>com.google.android.gms.permission.AD_ID<br>android.permission.FLASHLIGHT |

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。

## URL 链接安全分析

| URL信息 | 源码文件 |
| --- | --- |
| • http://aria.laoyuyu.me/aria_doc/api/use_broadcast.html | 自研引擎分析结果 |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
| --- | --- | --- |
| 岳鹰全景监控 | Alibaba | 岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。 |
| AntiFakerAndroidChecker | happylishang | Android 模拟器检测，检测 Android 模拟器，作为可信 DeviceID，应对防刷需求等。 |
| GlideWebpDecoder | zjupure | GlideWebpDecoder 是一个 Glide 集成库，用于在 Android 平台上解码和显示 webp 图像。它基于 libwebp 项目，并以 Fresco 和 GlideWebpSupport 的一些实现作为参考。 |
| Jetpack Camera | Google | CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。 |
| 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。 |

| | | |
|---|---|---|
| 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。 |

## 敏感凭证泄露检测

| 可能的密钥 |
|---|
| 友盟统计的 UMENG_CHANNEL: MIM18QS3 |
| YW5kcm9pZC5hcHAuQWN0aXZpdHlUaHJlYWQkUHJvdmlkZXJDbGllbnRSZWNvcmQ= |
| YW5kcm9pZC5hcHAuQWN0aXZpdHlUaHJlYWQkQXBwQmluZERhdGE= |

## 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，深入扫描软件中的潜在的漏洞和安全隐患。