南明离火

移动应用检测平台

# ANDROID 静态分析报告

北京中粮集团 • v5.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2024-03-22 10:18:09

# 应用概览

| | |
|---|---|
| 文件名称: | 北京中粮集团.apk |
| 文件大小: | 2.19MB |
| 应用名称: | 北京中粮集团 |
| 软件包名: | qfabw.vgtkel.jhgwrlf.nqhpdsza |
| 主活动: | minmtta.ewdygx.ahibyws.MainActivity |
| 版本号: | 5.0 |
| 最小SDK: | 21 |
| 目标SDK: | 29 |
| 加固信息: | 未加壳 |
| 应用程序安全分数: | 54/100 (中风险) |
| 杀软检测: | AI评估：安全 |
| MD5: | 0d1a91e5f5914cc0647480fa5052b541 |
| SHA1: | c91e2d09e42169117d42dc845de2b0322c519578 |
| SHA256: | e6d32c2cd41cc9eb33d12e3955fd9a1b9fe9d126c776be7b43690e52d38c20c |

## 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 1 | 3 | 1 | 1 | 0 |

## 四大组件导出状态统计

| |
|---|
| Activity组件：3个，其中export的有： 1个 |
| Service组件：1个，其中export的有： 0个 |
| Receiver组件：0个，其中export的有： 0个 |
| Provider组件：1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: False
v3 签名: False

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=0079082663, ST=keTlnPQHoI, L=xwNmgPfJMZ, O=EHPTOoyYWu, OU=WsiCkISnxp, CN=GMVHUatjZU
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-28 04:19:37+00:00
有效期至: 2047-06-22 04:19:37+00:00
发行人: C=0079082663, ST=keTlnPQHoI, L=xwNmgPfJMZ, O=EHPTOoyYWu, OU=WsiCkISnxp, CN=GMVHUatjZU
序列号: 0x553a1d6e
哈希算法: sha256
证书MD5: 38b4737decec3af5fd269255b017c0e4
证书SHA1: 500dd366bf1a0e6342a2a01d2144d1d3472c7ba2
证书SHA256: ab158d29960e19f1e3b2263577e28c16702c8e28273ea317dccfc7e2e3692663
证书SHA512:
1715bd969808421b14a9363c549425a5672c5a5670d4345983c7129a77d3a7563894878d3a48da6b1cccec1e6783192fc0dfa09ca3d2bac4023c1332c7a346e

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.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.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.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.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_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.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。 |

## 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: **1** | 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 |
| 应用程序存在Janus漏洞 | 高危 | 应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。 |

## Manifest 配置安全分析

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

高危: **0** | 警告: **3** | 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 | Activity-Alias (com.kmcjrz.bsesai.newActivity) 未被保护。存在一个intent-filter。 | 警告 | 发现 Activity-Alias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-Alias是显式导出的。 |

## 代码安全漏洞检测

高危: **0** | 警告: **0** | 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<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |

## 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） |
|---|---|---|---|---|---|---|---|---|---|

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | arm64-v8a/libomas.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 | 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: ['old_read_chk'] | False<br>warning<br>符号可用 |
| 2 | arm64-v8a/libscorpion.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。 | | False<br>high<br>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI | 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 | False<br>warning<br>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<br>info<br>符号被剥离 |

## 敏感权限滥用分析

| 类型 | 匹配 | 权限 |
|---|---|---|
| 恶意软件常用权限 | 2/30 | android.permission.CAMERA<br>android.permission.READ_PHONE_STATE |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | |
|---|---|---|
| 其它常用权限 | 5/46 | android.permission.INTERNET<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_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。

## 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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成