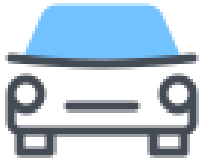
南明离火
移动应用检测平台

ANDROID 静态分析报告



Mahadev Car Rentals • v1.0

分析日期: 2024-02-19 21:38:26

应用概览

文件名称:	mahadev-car-rentals.apk
文件大小:	5.22MB
应用名称:	Mahadev Car Rentals
软件包名:	com.mahadev.carrentals
主活动:	com.mahadev.carrentals.MainActivity
版本号:	1.0
最小SDK:	14
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	38/100 (高风险)
杀软检测:	17 个杀毒软件报毒
MD5:	93234f87394478eac49e93a7e9f3afac
SHA1:	a7e3d4b492d86a7d13585bd06688cbda8070dfd4
SHA256:	c25f978301587136fe6e7af55[illegible]8c48ddd43212645[illegible]151156cbefe6

分析结果严重性分布

高危	中危	信息	安全	关注
4	6	1	1	0

四大组件导出状态统计

Activity组件：4个，其中export的有：0个
Service组件：1个，其中export的有：1个
Receiver组件：3个，其中export的有：3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
v4 签名: False
主题: CN=editor
签名算法: rsassa_pkcs1v15
有效期自: 2016-01-10 08:03:09+00:00
有效期至: 2115-12-17 08:03:09+00:00
发行人: CN=editor
序列号: 0x231bc320
哈希算法: sha256
证书MD5: cb3363348414b0583c830294c272e10f
证书SHA1: 927ca44949d7788aa86f9d7f04d7fdacecd1dfb9
证书SHA256: 6215f00baa4bf18bab5792fc796bfc5555917240f14f7c7e672d956888d75c96
证书SHA512:
c63cbae736201d74ed60e0ba1f252d598282fea1d64db0ee230a1e80fef2c0e25efa7fa6154e5dcfed4f5ec525e4b9591b47654078dbe67f3dlebc6d283e7e9a

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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。恶意程序会在用户未知的情况下监视或删除。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
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.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.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.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。
com.mahadev.cartoonals.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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

高危: **2** | 警告: **6** | 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 4.0-4.0.2, [minSdk=14]	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	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	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。
4	Activity (com.mahadev.carrentals.MainActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
5	Service (com.mahadev.carrentals.MyForeGroundService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
6	Broadcast Receiver (com.mahadev.carrentals.SmsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
7	Broadcast Receiver (com.mahadev.carrentals.MyBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
8	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: **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 OWASP MASVS: MSTG-STORAGE-3	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	5/30	android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.RECEIVE_BOOT_COMPLETED android.permission.CALL_PHONE
其它常用权限	2/46	android.permission.INTERNET android.permission.FOREGROUND_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
mahadevcarrentals.com	病毒 **URL:** mahadevcarrentals.com **IP:** N/A **Description:** Maltrail标记的恶意域	否	**IP地址:** 3.33.130.190 **国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://mahadevcarrentals.com/old_messages.php/	com/mahadev/carrentals/HomeActivity.java
• https://mahadevcarrentals.com/login.php	com/mahadev/carrentals/LoginActivity.java
• https://mahadevcarrentals.com/signup.php	com/mahadev/carrentals/SignupActivity.java
• https://mahadevcarrentals.com/send-sms.php • https://mahadevcarrentals.com/message.php	com/mahadev/carrentals/SmsReceiver.java

第三方 SDK 组件分析

本报告由南明离火移动安全分析平台生成

SDK名称	开发者	描述信息
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。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

免责声明及风险提示: