南明离火
移动应用检测平台

ANDROID 静态分析报告

ScooterHero • V1.2

本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-09 08:18:19

应用概览

文件名称:	ScooterHero v1.2.apk
文件大小:	2.32MB
应用名称:	ScooterHero
软件包名:	com.wuzla.game.ScooterHero_Paid
主活动:	com.wuzla.game.ScooterHero_Paid.paid.c.bfikaDwj
版本号:	1.2
最小SDK:	3
目标SDK:	3
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
杀软检测:	36 个杀毒软件报毒
MD5:	abe51091107424e66959a2cb8a716f2e
SHA1:	4ebd1e81c8e800ea20074fbc88f34aa6e145d3f3
SHA256:	724103a9f869148b332c184d8b9523f19a4f5d72623d97881206f6d90a50c2055

分析结果严重性

高危	中危	信息	安全	关注
3	10	1	1	0

四大组件信息

Activity组件：2个，其中export的有：1个
Service组件：1个，其中export的有：0个
Receiver组件：1个，其中export的有：1个
Provider组件：0个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: True

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=IT, ST=Unknown, L=Unknown, O=Obfuscapk, OU=Obfuscapk, CN=Obfuscapk
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-15 18:58:38+00:00
有效期至: 2049-08-07 18:58:38+00:00
发行人: C=IT, ST=Unknown, L=Unknown, O=Obfuscapk, OU=Obfuscapk, CN=Obfuscapk
序列号: 0x5f122eb3
哈希算法: sha256
证书MD5: 654f7f55899d0720aa524e768e0e98cf
证书SHA1: 09dceb70d91de79335b6c143d05f9a6b6de9e59c
证书SHA256: ed1399b288d3aac9ef9d43fcd9fbf90c7662b3ed0050b08f3c2988d24a8a42c9
证书SHA512:
348846cd1573e362aa88d7dc65ffc1b1c47cee87281355719db7f0c4c08c0d7f16ad1f581eb172fb2a5250680b7880ead3b0122c51064f381847de324e225e2

公钥算法: rsa
密钥长度: 2048
指纹: fbb4874e266f7bb91caf414a03f58255e03f169ab8a45998a39083de7a09990f
找到 1 个唯一证书

☰ 应用权限

权限名称	安全等级	权限内容	权限描述
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
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.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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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_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.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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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。
com.android.browser.permission.READ_HISTORY_BOOKMARKS	危险	获取自带浏览器上网记录	恶意代码可有利用此权限窃取用户的上网记录和书签。

com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	危险	修改自带浏览器上网记录	恶意代码可有利用此权限篡改用户的上网记录和书签。
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_GPS	签名(系统)	使用GPS权限	这个权限已经被废弃，不再被系统支持。这个权限曾经用于访问GPS位置，但是现在已经被android.permission.ACCESS_FINE_LOCATION替代。
android.permission.ACCESS_LOCATION	未知	未知权限	来自 android 引用的未知权限。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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分析

高危: **1** | 警告: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
3	Activity (ScooterHero_Paid) 未被保护。 存在一个intent-filter。	警告	发现 Activity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是显式导出的。

4	Broadcast Receiver (com.wuzla.game.ScooterHero_Paid.paid.f) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
5	高优先级的Intent （65535） - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

高危: **2** | 警告: **6** | 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
2	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
3	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
4	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
5	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
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 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

7	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
8	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
9	使用弱加密算法	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-4	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
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
00096	连接到 URL 并设置请求方法	命令 网络	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
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
00153	通过 HTTP 发送二进制数据	http	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
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限

00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00055	查询短信内容及电话号码来源	短信 信息收集	升级会员：解锁高级权限
00048	查询短信内容	短信 信息收集	升级会员：解锁高级权限
00049	查询短信发送者的电话号码	短信 信息收集	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
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
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
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
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
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
00007	Use absolute path of directory for the output media file path	文件	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
00193	发送短信	短信	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00074	获取 IMSI 和 ISO 国家代码	信息收集 电话服务	升级会员：解锁高级权限
00146	获取网络运营商名称和 IMSI	电话服务 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
00038	查询电话号码	信息收集	升级会员：解锁高级权限

00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	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
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
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00084	获取 ISO 国家代码和 IMSI	信息收集 电话服务	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.WRITE_CONTACTS android.permission.ACCESS_COARSE_LOCATION android.permission.RECEIVE_SMS android.permission.WRITE_SMS
其它常用权限	3/46	com.android.launcher.permission.INSTALL_SHORTCUT android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE

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链接分析

URL信息	源码文件
• 127.0.0.1	com/wuzla/game/ScooterHero_Paid/paid/e/q.java
• 127.0.0.1	com/wuzla/game/ScooterHero_Paid/paid/h.java

免责声明及风险提示: