南明离火
移动应用检测平台

ANDROID 静态分析报告

惠州车管 • v1.23

分析日期: 2024-06-07 12:01:02

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

应用概览

文件名称:	hzjg_qqtn.apk
文件大小:	2.53MB
应用名称:	惠州车管
软件包名:	com.uroad.hzcg
主活动:	com.uroad.hzcg.LoginActivity
版本号:	1.23
最小SDK:	10
目标SDK:	17
加固信息:	未加壳
应用程序安全分数:	37/100 (高风险)
跟踪器检测:	3/432
杀软检测:	1 个杀毒软件报毒
MD5:	a6bc9cfba25d3c0a2b92d54c9f3e452f
SHA1:	c1376101cc114fd5a994114593e57da3fe46f74b
SHA256:	2bf7c6584afb5c1afbb3f1ee458cd88e5b0e7a02a9beb4c30b507db6f2264d1e

分析结果严重性分布

高危	中危	信息	安全	关注
5	3	1	1	3

四大组件导出状态统计

Activity组件：16个，其中export的有：0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：0个，其中export的有：0个

应用签名证书信息

二进制文件已签名

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

v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=China, ST=gd, L=gz, O=uroad, OU=uroad, CN=uroad
签名算法: rsassa_pkcs1v15
有效期自: 2014-02-18 08:46:37+00:00
有效期至: 2114-01-25 08:46:37+00:00
发行人: C=China, ST=gd, L=gz, O=uroad, OU=uroad, CN=uroad
序列号: 0x4e75c928
哈希算法: sha256
证书MD5: be0f37ec16223f50c1a85bb51435ad2a
证书SHA1: d6cbf330e0fa15f4a5b6d3cd5c030fc833b16b4d
证书SHA256: e3959d7ff70ce7884604d63b1b8ef3bebc1de339fa98fd5f787dc897310efd62
证书SHA512:
893af2595fce63a1d8011dd61e66bfe17d299557cddf244a249d1bc0f5b9ad95d8fa9b5086b2512cbf38c8c2556cb837a9d401d3a4d1d9c750bec7c3d0a8040f

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.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.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_MOCK_LOCATION	危险	获取模拟定位信息	获取模拟定位信息，一般用于帮助开发者调试应用。恶意程序可以用它来覆盖真实位置信息源。
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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。

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

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: **1** | 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 2.3.3-2.3.7, [minSdk=10]	信息	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。
3	Activity (com.uroad.hzcg.LoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity （com.uroad.hzcg.LoginActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这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”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (17) 更新到 28 或更高版本以在平台级别修复此问题。

代码安全漏洞检测

高危: **2** | 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	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

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

2	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
3	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
5	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
6	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
7	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
8	使用了加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.RECORD_AUDIO android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.WRITE_SETTINGS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_MOCK_LOCATION android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.myapp.com	安全	是	**IP地址:** 101.89.47.26 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
cgi.qplus.com	安全	否	No Geolocation information available.
mta.oa.com	安全	否	**IP地址:** 141.144.196.217 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.jivesoftware.com	安全	否	**IP地址:** 23.235.209.143 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 弗吉尼亚海滩 **纬度:** 36.837925 **经度:** -76.093918 **查看:** Google 地图
jabber.org	安全	否	**IP地址:** 208.68.163.216 **国家:** 美利坚合众国 **地区:** 爱荷华州 **城市:** 蒙蒂塞洛 **纬度:** 42.238514 **经度:** -91.189705 **查看:** Google 地图

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

etherx.jabber.org	安全	否	**IP地址:** 208.68.163.210 **国家:** 美利坚合众国 **地区:** 爱荷华州 **城市:** 蒙蒂塞洛 **纬度:** 42.238514 **经度:** -91.189705 **查看:** Google 地图
oc.umeng.co	安全	否	No Geolocation information available.
www.weather.com.cn	安全	是	**IP地址:** 114.230.213.87 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
www.u-road.com	安全	是	**IP地址:** 47.96.92.29 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161530 **查看:** 高德地图
alog.umeng.co	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://cgi.qplus.com/report/report	com/tencent/utils/Util.java
• http://www.jivesoftware.com/xmlns/xmpp/properties	org/jivesoftware/smack/util/PacketParserUtils.java
• http://jabber.org/protocol/compress	org/jivesoftware/smack/XMPPConnection.java
• http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/utils/OpenConfig.java
• http://www.jivesoftware.com/xmlns/xmpp/properties	org/jivesoftware/smack/packet/Packet.java
• http://jabber.org/protocol/compress	org/jivesoftware/smack/PacketReader.java
• https://openmobile.qq.com/	com/tencent/utils/HttpUtils.java
• http://etherx.jabber.org/streams	org/jivesoftware/smack/PacketWriter.java

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

• http://qzs.qq.com • http://qzs.qq.com/open/mobile/not_support.html? • http://qzs.qq.com/open/mobile/request/sdk_request.html? • http://qzs.qq.com/open/mobile/invite/sdk_invite.html? • http://qzs.qq.com/open/mobile/reactive/sdk_reactive.html? • https://openmobile.qq.com/ • http://wspeed.qq.com/w.cgi • https://openmobile.qq.com/oauth2.0/m_authorize? • http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html? • http://qzs.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/utils/ServerSetting.java
• file:anonymous-string	com/hp/hpl/sparta/Parser.java
• http://connect.qq.com/ • http://www.qq.com/	com/uroad/util/QQWeiboUtil.java
• http://www.myapp.com/forward/a/45592?g_f=990935 • http://webpresence.qq.com/getonline?type=1&	com/tencent/wpa/WPA.java
• http://www.weather.com.cn/data/cityinfo/	com/uroad/common/BaseConstants.java
• http://www.u-road.com/	com/uroad/net/AsyncHttpClient.java
• https://graph.qq.com/weiyun/query_all_record • https://graph.qq.com/weiyun/check_record • https://graph.qq.com/weiyun/get_record • https://graph.qq.com/weiyun/create_record • https://graph.qq.com/weiyun/delete_record • https://graph.qq.com/weiyun/modify_record	com/tencent/weiyun/RecordManager.java
• http://106.187.97.123/androidapi/index.php?/log/cfor	com/uroad/webserverce/BaseWebService.java
• https://graph.qq.com/weiyun/upload_photo • https://graph.qq.com/weiyun/get_music_list • https://graph.qq.com/weiyun/delete_video • https://graph.qq.com/weiyun/delete_photo • https://graph.qq.com/weiyun/download_music • https://graph.qq.com/weiyun/upload_music • https://graph.qq.com/weiyun/get_photo_thumb • https://graph.qq.com/weiyun/delete_music • https://graph.qq.com/weiyun/upload_video • https://graph.qq.com/weiyun/get_photo_list • https://graph.qq.com/weiyun/download_photo • https://graph.qq.com/weiyun/get_video_list • https://graph.qq.com/weiyun/download_video	com/tencent/weiyun/FileManager.java

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

- https://graph.qq.com/weiyun/upload_photo
- http://www.jivesoftware.com/xmlns/xmpp/properties
- https://graph.qq.com/weiyun/get_music_list
- http://106.187.97.123/androidapi/index.php?/log/error
- https://graph.qq.com/weiyun/delete_photo
- https://graph.qq.com/weiyun/check_record
- https://graph.qq.com/weiyun/get_photo_thumb
- https://graph.qq.com/weiyun/delete_music
- https://graph.qq.com/weiyun/get_photo_list
- http://openmobile.qq.com/api/check2?page=qzshare.html&loginpage=loginindex.html&logintype=qzone
- https://graph.qq.com/weiyun/download_video
- http://qzs.qq.com/open/mobile/request/sdk_request.html?
- http://mta.qq.com/
- http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf
- javascript:window.jsbridge&&jsbridge.callback
- http://www.u-road.com/
- http://pingma.qq.com:80/mstat/report
- http://qzs.qq.com/open/mobile/invite/sdk_invite.html?
- https://graph.qq.com/weiyun/download_music
- 10.0.0.200
- http://jabber.org/protocol/compress'
- http://alog.umeng.co/app_logs
- http://fusion.qq.com/cgi-bin/qzapps/mapp_lbs_getnear.cgi
- https://graph.qq.com/weiyun/create_record
- http://webpresence.qq.com/getonline?type=1&
- http://wspeed.qq.com/w.cgi
- http://qzs.qq.com/open/mobile/rate/sdk_rate.html?
- http://mta.oa.com/
- http://qzs.qq.com/open/mobile/not_support.html?
- http://connect.qq.com/
- http://www.qq.com/
- https://openmobile.qq.com/user/user_login_statis
- http://appact.qzone.qq.com/appstore_activity_task_pcpush_sdk
- https://graph.qq.com/weiyun/query_all_record
- https://graph.qq.com/weiyun/delete_video
- http://www.weather.com.cn/data/cityinfo/
- http://qzs.qq.com/open/mobile/reactive/sdk_reactive.html?
- https://graph.qq.com/weiyun/upload_video
- https://graph.qq.com/weiyun/download_photo
- http://fusion.qq.com/cgi-bin/qzapps/mapp_lbs_delete.cgi
- http://openmobile.qq.com/api/check?page=shareindex.html&style=9
- https://graph.qq.com/weiyun/get_video_list
- http://oc.umeng.co/check_config_update
- http://etherx.jabber.org/streams
- file:anonymous-strin
- https://openmobile.qq.com/oauth2.0/m_authorize?
- https://graph.qq.com/weiyun/delete_record
- http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?
- https://graph.qq.com/weiyun/modify_record
- http://qzs.qq.com/open/mobile/brag/sdk_brag.html?
- http://www.myapp.com/forward/a/4585?g_f=990935
- http://qzs.qq.com
- http://cgi.qplus.com/report/report
- http://cgi.connect.qq.com/qqconnectutil/sdk
- http://www.weather.com.cn/m/i/icon_weather/42x30/
- https://graph.qq.com/weiyun/get_record
- http://jabber.org/protocol/compress
- https://graph.qq.com/weiyun/upload_music
- https://openmobile.qq.com/
- http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi
- 10.0.0.172

自研引擎-S

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

第三方 SDK 组件分析

SDK名称	开发者	描述信息
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
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。

第三方追踪器检测

名称	类别	网址
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Tencent Weiyun		https://reports.exodus-privacy.eu.org/trackers/117
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "5306f28156240b6f9f242ec0"
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
36f68aba34db77ac54d27e66fec00c51e805e5d5
5302fe4256240b6fa4009a78
d8391a394d4a179e6fe7bdb8a301258b
boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
e390a4bcccc81165bd4bc9d94d47eabb2c47d691
160e7bd42dec9428721034e0116fc6dd

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

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