MOBSF

ANDROID STATIC ANALYSIS REPORT

Wheelmap (5.3)

File Name:	Wheelmap_5.3_APKPure.apk
Package Name:	org.wheelmap.android.online
Scan Date:	Nov. 23, 2024, 4:22 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	4	1	1	1

FILE INFORMATION

File Name: Wheelmap_5.3_APKPure.apk
Size: 2.73MB
MD5: 1681e407b7862bdb1ff18a111a2d4cab
SHA1: e2ecd832b5feaa77b902f8f27587e6c4f5e3cf27
SHA256: 4af84afa179fa391dafb0ef3224edfb59caa5a794a56a042235144126091ae9d

APP INFORMATION

App Name: Wheelmap
Package Name: org.wheelmap.android.online
Main Activity: org.wheelmap.pwawrapper.MainActivity
Target SDK: 31
Min SDK: 21
Max SDK:
Android Version Name: 5.3
Android Version Code: 500026

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=DE, ST=Berlin, L=Berlin, O=Sozialhelden, OU=Sozialhelden, CN=Christoph B√ºnte
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-15 13:57:10+00:00
Valid To: 2039-07-03 13:57:10+00:00
Issuer: C=DE, ST=Berlin, L=Berlin, O=Sozialhelden, OU=Sozialhelden, CN=Christoph B√ºnte
Serial Number: 0x4f3bb9b6
Hash Algorithm: sha1
md5: 296692ba3c2cdb7d244bff3aedbe0e3e
sha1: 41a62d449d25d967eb620635e6b25f9a937f99be
sha256: d519970a284b043bfb5cb02460887a426b0e0482c4ed70605f131cee9372d8ed
sha512: 3c2b92de10215e459c5a9c2c1484f395d708bb3dd938e4c2acac7246dfe77d41def5f72cb38f4bcd40a4f4243ea53bad6e5497470ce8bc4d868cf3c1ffd9e9bc
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 33380042a73cfefc5aeb1160859388095df78efc490430f90881b6f1c9723e69
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.wheelmap.pwawrapper.MainActivity	Schemes: http://, https://, Hosts: wheelmap.org, Path Prefixes: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

CODE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	org/wheelmap/pwawrapper/Configuration.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/wheelmap/pwawrapper/webview/WebViewHelper.java
3	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	org/wheelmap/pwawrapper/MainActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	org/wheelmap/pwawrapper/webview/WebViewHelper.java
00022	Open a file from given absolute path of the file	file	org/wheelmap/pwawrapper/webview/WebViewHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	org/wheelmap/pwawrapper/webview/WebViewHelper.java
00036	Get resource file from res/raw directory	reflection	org/wheelmap/pwawrapper/webview/WebViewHelper.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA
Other Common Permissions	0/44	

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

PLAYSTORE INFORMATION

Title: Wheelmap

Score: 3.173913 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Travel & Local **Play Store URL:** org.wheelmap.android.online

Developer Details: SOZIALHELDEN e.V., SOZIALHELDEN+e.V., None, http://sozialhelden.de, info@sozialhelden.de,

Release Date: Mar 14, 2012 **Privacy Policy:** Privacy link

Description:

Find and rate wheelchair accessible places – worldwide and free of charge. Find wheelchair accessible restaurants, cafes, toilets, shops, cinemas, parking lots, bus stops and much more. The Wheelmap and OpenStreetMap communities have already rated about 1 million places! Ratings for another million places come from a growing number of partners such as Foursquare City Guide, Jaccede, AXSMap, HERE, Parkopedia, bahnhof.de, Mapy bez barier, etc. All in all, you can find accessibility reviews of more than 2,000,000 places on Wheelmap! More entries are added daily. As with Wikipedia, you too can join in and contribute information about places worldwide. This is important, because in some regions of the world there are only a few entries at the moment. Help us improve the map: Rate the entrances and restrooms of public places according to their wheelchair accessibility and upload images of the places. The 30 countries with the highest number of rated places are: Germany (582,174), United States (277,194), India (258,992), France (161,486), South Africa (74,568), Canada (57,247), Czech Republic (53,888) United Kingdom (53,718), Austria (52,253), Italy

(40,256), Australia (31,238), Spain (25,905), Algeria (24,657), Japan (21,503), Switzerland (20,820), Taiwan (15,300), Netherlands (15,030), Russian Federation (13,816), Hungary (13,186), Poland (13,056), United Arab Emirates (12,976), Turkey (11,180), Belgium (8,834), Brazil (8,070), Indonesia (7,765), Ukraine (7,495), Republic of Côte d'Ivoire (7,467), Mexico (7,449), Croatia (7,194). Wheelmap is available in 32 languages. Your smartphone must be set to one of the following languages: Arabic Bulgarian Catalan Chinese (Taiwan) Chinese (Traditional) Chinese (Simplified) Czech Danish Dutch English (United States) Finnish French German Greek Hebrew Hindi Hungarian Italian Japanese Korean Norwegian Polish Portuguese Portuguese (Brazil) Romanian Russian Slovak Spanish Swedish Turkish Ukrainian Vietnamese

SCAN LOGS

Timestamp	Event	Error
2024-11-23 04:22:17	Generating Hashes	OK
2024-11-23 04:22:17	Extracting APK	OK
2024-11-23 04:22:17	Unzipping	OK
2024-11-23 04:22:17	Getting Hardcoded Certificates/Keystores	OK
2024-11-23 04:22:17	Parsing APK with androguard	OK
2024-11-23 04:22:20	Parsing AndroidManifest.xml	OK
2024-11-23 04:22:20	Extracting Manifest Data	OK

2024-11-23 04:22:20	Manifest Analysis Started	OK
2024-11-23 04:22:20	Performing Static Analysis on: Wheelmap (org.wheelmap.android.online)	OK
2024-11-23 04:22:20	Fetching Details from Play Store: org.wheelmap.android.online	OK
2024-11-23 04:22:20	Checking for Malware Permissions	OK
2024-11-23 04:22:20	Fetching icon path	OK
2024-11-23 04:22:20	Library Binary Analysis Started	OK
2024-11-23 04:22:20	Reading Code Signing Certificate	OK
2024-11-23 04:22:21	Running APKiD 2.1.5	OK
2024-11-23 04:22:22	Detecting Trackers	OK
2024-11-23 04:22:23	Decompiling APK to Java with JADX	OK

2024-11-23 04:22:41	Converting DEX to Smali	OK
2024-11-23 04:22:41	Code Analysis Started on - java_source	OK
2024-11-23 04:22:43	Android SAST Completed	OK
2024-11-23 04:22:43	Android API Analysis Started	OK
2024-11-23 04:22:45	Android API Analysis Completed	OK
2024-11-23 04:22:45	Android Permission Mapping Started	OK
2024-11-23 04:22:47	Android Permission Mapping Completed	OK
2024-11-23 04:22:47	Android Behaviour Analysis Started	OK
2024-11-23 04:22:49	Android Behaviour Analysis Completed	OK
2024-11-23 04:22:49	Extracting Emails and URLs from Source Code	OK
2024-11-23 04:22:49	Email and URL Extraction Completed	OK

2024-11-23 04:22:49	Extracting String data from APK	OK
2024-11-23 04:22:49	Extracting String data from Code	OK
2024-11-23 04:22:49	Extracting String values and entropies from Code	OK
2024-11-23 04:22:50	Performing Malware check on extracted domains	OK
2024-11-23 04:22:51	Saving to Database	OK

Report Generated by - MobSF v4.2.4

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.