MOBSF

ANDROID STATIC ANALYSIS REPORT

fuelService (24.10.07)

File Name:	fuelService.apk
Package Name:	org.fuelservice.app
Scan Date:	Nov. 17, 2024, 8:22 p.m.
App Security Score:	62/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	4	1	2	1

FILE INFORMATION

File Name: fuelService.apk
Size: 6.19MB
MD5: dbca996ae1d7beb82250c9d27ac9b8e0
SHA1: fbabf629c28e6f07b33d4c269ecb8534d824daeb
SHA256: 14e37675e99f0fae03db7785db43de0bf5b7a658044184463c2d1228f84cf5f2

APP INFORMATION

App Name: fuelService
Package Name: org.fuelservice.app
Main Activity: org.fuelservice.app.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 24.10.07
Android Version Code: 241007

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 2
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=gb, ST=lancashire, L=orrell, O=fuelservice, OU=fuelservice, CN=fuel service
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-04-28 23:46:58+00:00
Valid To: 2042-09-13 23:46:58+00:00
Issuer: C=gb, ST=lancashire, L=orrell, O=fuelservice, OU=fuelservice, CN=fuel service
Serial Number: 0x30b0cb84
Hash Algorithm: sha256
md5: 085ea8f4575ac4c9663c2a073c2635c0
sha1: 7a54ce1f06c91e58260a0feb1ad962cb0fc20100
sha256: 7acdbba2d9352f7a536241041b6dc77947c9aab0e2a29daab8dd69ce308ed7de
sha512: ac08326c541f135a6f2ecc388289aafa129dd1fd28a7e4a3765ddbbc7dc2498a79da1b715a82d79a2afa112069d2b5d5ec86a69533f216b4c175bbcffd3ba722
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b37d8d9a1171060a6a45b2e9b9ff9eb2d88de07d5a92714ea6c4c28a9152bd62
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_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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
org.fuelservice.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.fuelservice.app.MainActivity	Schemes: fuelservice://, ://, Hosts: , Path Prefixes: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | 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.

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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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: 0 | WARNING: 2 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	cordova/plugins/Diagnostic.java
2	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	com/badrit/Backbutton/BackbuttonPlugin.java com/customtabplugin/ChromeCustomTabPlugin.java com/lampa/startapp/Assets.java cordova/plugins/Diagnostic.java cordova/plugins/Diagnostic_Bluetooth.java cordova/plugins/Diagnostic_Camera.java cordova/plugins/Diagnostic_External_Storage.java cordova/plugins/Diagnostic_Location.java cordova/plugins/Diagnostic_NFC.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/Diagnostic_Wifi.java defpackage/Crypto.java defpackage/NativeStorage.java uk/co/workingedge/phonegap/plugin/CordovaLogger.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java uk/co/workingedge/phonegap/plugin/LaunchReview.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cordova/plugins/Diagnostic.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.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	com/customtabplugin/ChromeCustomTabPlugin.java com/lampa/startapp/startApp.java cordova/plugins/Diagnostic_Notifications.java uk/co/workingedge/LaunchNavigator.java uk/co/workingedge/phonegap/plugin/LaunchReview.java
00091	Retrieve data from broadcast	collection	com/lampa/startapp/startApp.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/customtabplugin/ChromeCustomTabPlugin.java com/lampa/startapp/startApp.java cordova/plugins/Diagnostic_Notifications.java uk/co/workingedge/LaunchNavigator.java
00013	Read file and put it into a stream	file	okio/Okio.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	cordova/plugins/Diagnostic.java
00036	Get resource file from res/raw directory	reflection	com/customtabplugin/ChromeCustomTabPlugin.java cordova/plugins/Diagnostic_Notifications.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE
Other Common Permissions	1/44	android.permission.BLUETOOTH

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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	**IP:** 172.217.1.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
share.here.com	ok	**IP:** 13.33.165.25 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
citymapper.com	ok	**IP:** 141.101.90.105 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

PLAYSTORE INFORMATION

Title: fuelService

Score: 3.875 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** org.fuelservice.app

Developer Details: Fuel Service, 4670222918910919017, None, https://fuelservice.org, info@fuelservice.org,

Release Date: Apr 29, 2015 **Privacy Policy:** Privacy link

Description:

*Find Petrol Stations Near You Wherever you are, find a station near your current location, by distance or on a map *Know Before You Go Contact the petrol station before you go there to ask them if they can assist, don't waste time going to stations that can't help *Tell Them You Have Arrived Tells the petrol station you have arrived and they can respond by letting you know how long they will be *Rate and Review Give the station a rating and review so others can see and they can improve if necessary

SCAN LOGS

Timestamp	Event	Error
2024-11-17 20:22:45	Generating Hashes	OK

2024-11-17 20:22:45	Extracting APK	OK
2024-11-17 20:22:45	Unzipping	OK
2024-11-17 20:22:45	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 20:22:45	Parsing APK with androguard	OK
2024-11-17 20:22:46	Parsing AndroidManifest.xml	OK
2024-11-17 20:22:46	Extracting Manifest Data	OK
2024-11-17 20:22:46	Performing Static Analysis on: fuelService (org.fuelservice.app)	OK
2024-11-17 20:22:46	Fetching Details from Play Store: org.fuelservice.app	OK
2024-11-17 20:22:46	Manifest Analysis Started	OK
2024-11-17 20:22:46	Checking for Malware Permissions	OK
2024-11-17 20:22:46	Fetching icon path	OK

2024-11-17 20:22:46	Library Binary Analysis Started	OK
2024-11-17 20:22:46	Reading Code Signing Certificate	OK
2024-11-17 20:22:46	Running APKiD 2.1.5	OK
2024-11-17 20:22:48	Detecting Trackers	OK
2024-11-17 20:22:48	Decompiling APK to Java with JADX	OK
2024-11-17 20:22:54	Converting DEX to Smali	OK
2024-11-17 20:22:54	Code Analysis Started on - java_source	OK
2024-11-17 20:22:54	Android SAST Completed	OK
2024-11-17 20:22:54	Android API Analysis Started	OK
2024-11-17 20:22:54	Android API Analysis Completed	OK
2024-11-17 20:22:55	Android Permission Mapping Started	OK

2024-11-17 20:22:57	Android Permission Mapping Completed	OK
2024-11-17 20:22:57	Email and URL Extraction Completed	OK
2024-11-17 20:22:57	Android Behaviour Analysis Started	OK
2024-11-17 20:22:57	Android Behaviour Analysis Completed	OK
2024-11-17 20:22:57	Extracting String data from APK	OK
2024-11-17 20:22:57	Extracting String data from Code	OK
2024-11-17 20:22:57	Extracting String values and entropies from Code	OK
2024-11-17 20:22:58	Performing Malware check on extracted domains	OK
2024-11-17 20:22:58	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.