ANDROID STATIC ANALYSIS REPORT

OpenVegeMap (1.0.0)

File Name:	pro.rudloff.openvegemap_10001.apk
Package Name:	pro.rudloff.openvegemap
Scan Date:	May 22, 2022, 2:03 p.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	1	1	1	1

FILE INFORMATION

File Name: pro.rudloff.openvegemap_10001.apk
Size: 2.69MB
MD5: 84503126dbe6211d7b37a9c7ac391658
SHA1: fc27e0724f4c2bd7be629fb94d2c1e2ab7ccdfe0
SHA256: 67494f8e4b5020a6ac91128d957ee4b91da8a32fe6d812b2577efa12ebe81af0

APP INFORMATION

App Name: OpenVegeMap
Package Name: pro.rudloff.openvegemap
Main Activity: pro.rudloff.openvegemap.MainActivity
Target SDK: 27
Min SDK: 19
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 10001

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-05-07 08:03:46+00:00
Valid To: 2045-09-22 08:03:46+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x237af11f
Hash Algorithm: sha256
md5: 8abc83220ceabd62a65162581da4fe24
sha1: 65221d6bef254cdb7643c220614f90b432bc7a82
sha256: 5c50df068fa8b85c6033dc2bce15d0eb13225411f8385bb854540893e6870f43
sha512: 936f6dccf48aa25fa080afdf96a32c68385e34b124f9a7ca5a14306c32ef44ee08af1db9d887447f97ef0c95e91a87751f53c99a6b08531c539aa04dac4cab8e

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

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.

APKID ANALYSIS

FILE	DETAILS

<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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
pro.rudloff.openvegemap.MainActivity	Schemes: https://, http://, Hosts: openvegemap.netlib.re,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Launch Mode of Activity (pro.rudloff.openvegemap.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

CODE ANALYSIS

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	com/nordnetab/cordova/ul/UniversalLinksPlugin.java com/nordnetab/cordova/ul/model/JSMessage.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
9	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

Report Generated by - MobSF v3.5.2 Beta

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.