ANDROID STATIC ANALYSIS REPORT

WiGLE WiFi Wardriving FOSS (2.10)

File Name:	installer218.apk
Package Name:	net.wigle.wigleandroid
Scan Date:	May 31, 2022, 3:46 p.m.
App Security Score:	**28/100 (CRITICAL RISK)**
Grade:	F

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	5	1	1	2

FILE INFORMATION

File Name: installer218.apk
Size: 1.63MB
MD5: 1c1640bec77e5b6130e44d735e2ca986
SHA1: 62fea450484adbf139e3f08578eabf7f5e26d524
SHA256: 8726ca23ec76ef917a8b2b329b7871e4bb772ca533ff530e6ccd537d8cf63d23

APP INFORMATION

App Name: WiGLE WiFi Wardriving FOSS
Package Name: net.wigle.wigleandroid
Main Activity: net.wigle.wigleandroid.MainActivity
Target SDK: 23
Min SDK: 9
Max SDK:
Android Version Name: 2.10
Android Version Code: 210

APP COMPONENTS

Activities: 5
Services: 1
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: 2012-10-16 19:34:54+00:00
Valid To: 2040-03-03 19:34:54+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x507db6de
Hash Algorithm: sha1
md5: 38cfa1cfc1eeac453cb23dc53fc7d85d
sha1: 82f4cb091bbde751f99e69ef358877d6a767b721
sha256: 699dbee594797d7efb681f625620ec1e41e41e6a57afdcd8533f8d22003529e8
sha512: a5900490f923eec41d9aab473771f6675660e302ec10addb9cfe5acf7303633bac338832dd68e6c48fde0bf4b3e0e9c288671812c6235ee4ab1b243e474629ad
```

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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_MOCK_LOCATION	dangerous	mock location sources for testing	Create mock location sources for testing. Malicious applications can use this to override the location and/or status returned by real-location sources such as GPS or Network providers.

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

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-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.PRODUCT check
Build.BOARD check
network operator name 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>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Launch Mode of Activity (net.wigle.wigleandroid.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.
3	Launch Mode of Activity (net.wigle.wigleandroid.ErrorReportActivity) 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.
4	Launch Mode of Activity (net.wigle.wigleandroid.SpeechActivity) 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.
5	Launch Mode of Activity (net.wigle.wigleandroid.NetworkActivity) 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.
6	Launch Mode of Activity (net.wigle.wigleandroid.DBResultActivity) 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	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	net/wigle/wigleandroid/background/FileUploaderTask.java net/wigle/wigleandroid/DatabaseHelper.java net/wigle/wigleandroid/ErrorReportActivity.java net/wigle/wigleandroid/MainActivity.java
2	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	net/wigle/wigleandroid/NetworkActivity.java net/wigle/wigleandroid/ListFragment.java net/wigle/wigleandroid/SiteStatsFragment.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	net/wigle/wigleandroid/background/QueryThread.java net/wigle/wigleandroid/DatabaseHelper.java
4	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	net/wigle/wigleandroid/MainActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.opengis.net	ok	**IP:** 66.244.86.70 **Country:** United States of America **Region:** Indiana **City:** Jasper **Latitude:** 38.391441 **Longitude:** -86.931107 **View:** Google Map
wigle.net	ok	**IP:** 54.70.85.50 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
maps.google.com	ok	**IP:** 216.58.208.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.wigle.net	ok	**IP:** 54.70.85.50 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

EMAILS

EMAIL	FILE
bobzilla@wigle.net	net/wigle/wigleandroid/ErrorReportActivity.java

HARDCODED SECRETS

POSSIBLE SECRETS
"crypto_password" : "Password"
"crypto_password" : "Password"
"crypto_password" : "パスワード"
"crypto_show_password" : "パスワードを表示します。"
"setting_show_password" : "パスワードを表示する"
"status_no_user" : "ユーザ名が設定されていません"
"crypto_password" : "Passwort"
"crypto_password" : "סיסמה"
"crypto_password" : "密碼"

POSSIBLE SECRETS
"crypto_show_password" : "顯示密碼。"
"password" : "WiGLE密碼"
"setting_show_password" : "顯示密碼"
"status_no_user" : "用戶名不設定"
"username" : "WiGLE名"
"crypto_password" : "Salasana"
"crypto_password" : "पासवर्ड"
"crypto_password" : "Wachtwoord"
"password" : "WiGLE-wachtwoord"
"username" : "WiGLE-gebruikersnaam"
"crypto_password" : "Hasło"
"crypto_password" : "Password"
"crypto_password" : "암호"
"crypto_password" : "Passord"
"crypto_password" : "Password"

POSSIBLE SECRETS
"crypto_password" : "Parola"
"crypto_password" : "Heslo"
"crypto_password" : "Contraseña"
"password" : "Contraseña"
"crypto_password" : "Password"
"crypto_password" : "Senha"
"crypto_password" : "Jelszó"
"crypto_password" : "Пароль"
"crypto_password" : "Lösenord"
"crypto_password" : "Wachtwurd"
"password" : "WiGLE-wachtwurd"
"username" : "WiGLE-brûkersnamme"
"crypto_password" : "Senha"

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.