MOBSF

ANDROID STATIC ANALYSIS REPORT

RadioBeacon (0.8.18)

File Name:	installer336.apk
Package Name:	org.openbmap
Scan Date:	May 31, 2022, 12:47 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	12	1	1	1

FILE INFORMATION

File Name: installer336.apk
Size: 1.77MB
MD5: fa1189cbab1b16dde04b49989d56974c
SHA1: edd8cf1d63610ac7ec35ccf3573cd8e978e130e9
SHA256: 5657978156dcd8f9261ec5b1b692cd1fbfa3cb6f30b7c347b11ae0d57b5b362f

APP INFORMATION

App Name: RadioBeacon
Package Name: org.openbmap
Main Activity: org.openbmap.activities.StartscreenActivity
Target SDK: 23
Min SDK: 13
Max SDK:
Android Version Name: 0.8.18
Android Version Code: 27

APP COMPONENTS

Activities: 14
Services: 4
Receivers: 0
Providers: 1
Exported Activities: 3
Exported Services: 1
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: 2013-08-25 16:38:47+00:00
Valid To: 2041-01-10 16:38:47+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5558c077
Hash Algorithm: sha256
md5: 7d7b10894daf3c4d83c94c5e7b083b6d
sha1: fece4544487fe03d42267a558969acfc026d4e6e
sha256: a9d48266b3eb4a71474eebe3658a956d170b762642c98b419c6029c969851af6
sha512: 8a671c2c9f959057fdd7219cec7e8a11debf91d751b2004c188f473d079be72ba5ce6367d4ef76f036a811c5d83c5a50052b01febeb412952d9520d755f565b2

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.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_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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti-VM Code: Build.MANUFACTURER check Compiler: dx

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	Activity (org.openbmap.commands.StartTracking) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
3	Activity (org.openbmap.commands.StopTracking) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Activity (org.openbmap.commands.UploadAll) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
5	Service (org.openbmap.services.MasterBrainService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/openbmap/c/e.java org/openbmap/activities/ai.java org/openbmap/activities/StartscreenActivity.java org/openbmap/activities/bf.java org/openbmap/services/positioning

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/openbmap/services/positioning/PositioningService.java org/openbmap/activities/s.java org/openbmap/activities/x.java org/openbmap/activities/t.java org/openbmap/c/n.java org/openbmap/c/a.java org/openbmap/db/ContentProvider.java org/openbmap/services/wireless/c.java org/openbmap/activities/MapViewActivity.java org/openbmap/db/c.java org/openbmap/activities/CreditsActivity.java org/openbmap/activities/b.java org/openbmap/utils/aj.java com/a/a/cq.java org/openbmap/db/a.java org/openbmap/activities/ag.java org/openbmap/utils/af.java org/openbmap/c/l.java org/openbmap/services/positioning/a/a.java org/openbmap/services/wireless/b.java org/openbmap/activities/DialogPreferenceMaps.java com/a/a/a.java org/openbmap/services/MasterBrainService.java org/openbmap/c/i.java org/openbmap/services/wireless/a/e.java org/openbmap/c/d.java org/openbmap/services/wireless/WirelessLoggerService.java org/openbmap/c/k.java org/openbmap/activities/y.java org/openbmap/activities/CellDetailsMap.java org/openbmap/activities/TabHostAc

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	tivity.java org/openbmap/activities/WifiDetailsActivity.java org/openbmap/services/f.java com/a/a/cd.java org/openbmap/activities/n.java org/openbmap/activities/DialogPreferenceCatalogs.java org/openbmap/services/c.java org/openbmap/services/a.java org/openbmap/utils/ao.java org/openbmap/utils/r.java org/openbmap/activities/WifiDetailsMap.java org/openbmap/utils/i.java org/openbmap/activities/av.java com/jjoe64/graphview/o.java org/openbmap/utils/k.java org/openbmap/activities/StatusBar.java org/openbmap/b/b.java org/openbmap/services/positioning/GpxLoggerService.java org/openbmap/services/wireless/a/d.java org/openbmap/services/e.java org/openbmap/activities/SelectiveScrollViewPager.java org/openbmap/services/wireless/d.java org/openbmap/services/positioning/c.java org/openbmap/utils/aa.java org/openbmap/activities/bm.java org/openbmap/utils/l.java org/openbmap/activities/SettingsActivity.java org/openbmap/activities/bl.java org/openbmap/activities/bh.java org/openbmap/utils/VerticalLabelView.java org/openbmap/utils/ab.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/openbmap/db/a/g.java org/openbmap/services/wireless/a/b.java org/openbmap/utils/aq.java org/a/a/c.java org/openbmap/db/b.java org/xmlpull/v1/XmlPullParserException.java org/openbmap/activities/StatsActivity.java org/a/a/b.java org/openbmap/activities/aq.java org/openbmap/services/d.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	org/mapsforge/a/c/h.java
3	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	org/openbmap/activities/bf.java org/openbmap/db/c.java org/openbmap/activities/b.java org/openbmap/db/a.java org/openbmap/services/wireless/WirelessLoggerService.java org/openbmap/utils/ao.java org/openbmap/utils/r.java org/openbmap/utils/k.java org/openbmap/utils/aa.java
4	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	org/openbmap/db/ContentProvider.java org/openbmap/db/c.java org/openbmap/db/a.java org/openbmap/services/wireless/WirelessLoggerService.java org/openbmap/activities/WifiDetailsActivity.java org/openbmap/utils/k.java org/openbmap/utils/aq.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	org/mapsforge/map/c/b/a/a.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/openbmap/utils/l.java
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/openbmap/db/a/g.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 use no DRBG functionality for its cryptographic operations.
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'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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.
9	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.
10	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
11	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
12	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.dsb.dk	ok	**IP:** 13.107.213.67 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.179.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
barcelonabusturistic.cat	ok	**IP:** 63.33.124.79 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
www.topografix.com	ok	**IP:** 104.209.197.87 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
radiocells.org	ok	**IP:** 94.79.179.26 **Country:** Germany **Region:** Rheinland-Pfalz **City:** Kerpen **Latitude:** 50.309669 **Longitude:** 6.729780 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
wifi@boreal.no wifi@nettbuss.no	org/openbmap/services/wireless/a/e.java

HARDCODED SECRETS

POSSIBLE SECRETS
"prefs_credentials" : "Credentials"
"prefs_credentials_password" : "Password"
"prefs_credentials_password_summary" : ""
"prefs_credentials_user" : "Login"

POSSIBLE SECRETS
"sessions" : "Sessions"
"prefs_credentials" : "Legitimationsoplysninger"
"prefs_credentials_password" : "Adgangskode"
"prefs_credentials_password_summary" : "Adgangskoder:"
"sessions" : "Sessioner"
"dialog_delete_all_sessions_title" : "すべてのセッションを削除しますか?"
"do_you_want_to_delete_processed_sessions" : "アップロードしたセッションを削除しますか?"
"prefs_auto_delete_sessions_title" : "古いセッションをクリーンアップ"
"prefs_credentials" : "資格情報"
"prefs_credentials_anonymous_upload" : "匿名のアップロード"
"prefs_credentials_anonymous_upload_summary" : "匿名のアップロードを有効にします"
"prefs_credentials_password" : "パスワード"
"prefs_credentials_password_summary" : "パスワード:"
"prefs_credentials_user" : "ログイン"
"sessions" : "セッション"
"warning_bad_password" : "ユーザー名またはパスワードが間違っています!"

POSSIBLE SECRETS
"prefs_credentials" : "Login-Daten"
"prefs_credentials_password" : "Passwort"
"prefs_credentials_user" : "User"
"sessions" : "Sitzungen"
"prefs_credentials_password" : "Wachtwoord"
"prefs_credentials_password_summary" : ""
"prefs_credentials_user" : "Login"
"prefs_credentials_password" : "Hasło"
"prefs_credentials_user" : "Użytkownik"
"sessions" : "Sesje"
"prefs_credentials" : "Credenciales"
"prefs_credentials_password" : "Contraseña"
"sessions" : "Sesiones"
"prefs_credentials" : "Credenziali"
"prefs_credentials_password" : "Password"
"prefs_credentials_password_summary" : "Password:"

POSSIBLE SECRETS
"prefs_credentials_user" : "Login"
"sessions" : "Sessioni"
"prefs_credentials_password" : "Jelszó"
"prefs_credentials_password_summary" : "Jelszavak:"
"prefs_credentials_user" : "Felhasználónév"
"sessions" : "Munkamenetek"
"dialog_delete_all_sessions_title" : "删除全部会话？"
"do_you_want_to_delete_processed_sessions" : "您要删除已上传的会话？"
"prefs_auto_delete_sessions_title" : "清理旧会话"
"prefs_credentials" : "证书"
"prefs_credentials_anonymous_upload" : "匿名上传"
"prefs_credentials_anonymous_upload_summary" : "激活匿名上传"
"prefs_credentials_password" : "密码"
"prefs_credentials_password_summary" : "密码："
"prefs_credentials_user" : "登录"
"sessions" : "会话"

POSSIBLE SECRETS
"warning_bad_password" : "用户名或密码错误！"
"prefs_credentials" : "憑據"
"prefs_credentials_password" : "密碼"
"prefs_credentials_user" : "登入"

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.