

ANDROID STATIC ANALYSIS REPORT



Radiobeacon (0.8.15)

File Name:	installer347.apk
Package Name:	org.openbmap
Scan Date:	May 31, 2022, 2:33 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	12	1	1	1

FILE INFORMATION

File Name: installer347.apk

Size: 1.52MB

MD5: df8c71c5dfee2e760bd57cba2e1895c3

SHA1: a368df5d18adae762aa08337899bbd0bacba1009

SHA256: c99e4deb235b1b8492ee7aff682cb264c9ce053a39f19e1057f3e73c18edac26

i APP INFORMATION

App Name: Radiobeacon
Package Name: org.openbmap

Main Activity: org.openbmap.activities.StartscreenActivity

Target SDK: 19 Min SDK: 13 Max SDK:

Android Version Name: 0.8.15 Android Version Code: 24

EE APP COMPONENTS

Activities: 14 Services: 4 Receivers: 0 Providers: 1

Exported Activities: 3 Exported Services: 1 Exported Receivers: 0 Exported Providers: 0



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

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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

M APKID ANALYSIS

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

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

Q 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/services/wireless/a/d.java org/openbmap/c/g.java org/openbmap/activities/Startscre enActivity.java org/openbmap/services/c.java org/openbmap/bd/a.java org/openbmap/activities/am.java org/openbmap/activities/am.java org/openbmap/activities/am.java org/openbmap/activities/mapView Activity.java org/xmlpull/v1/XmlPullParserExce ption.java org/openbmap/services/positionin g/GpxLoggerService.java org/openbmap/services/MasterBr ainService.java org/openbmap/activities/ag.java org/openbmap/activities/ak.java org/openbmap/activities/DialogPr eferenceMaps.java org/openbmap/c/d.java org/openbmap/c/d.java org/openbmap/services/wireless/ d.java com/a/a/a.java org/openbmap/services/positionin g/c.java org/openbmap/services/positionin g/c.java org/openbmap/services/positionin g/c.java org/openbmap/services/f.java org/openbmap/services/f.java org/openbmap/services/f.java org/openbmap/services/f.java org/openbmap/services/f.java org/openbmap/activities/y.java org/openbmap/activities/y.java org/openbmap/activities/y.java

NO	ISSUE	SEVERITY	STANDARDS	IsMap.java File/bSenbmap/services/a.java
NO 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	
				g/PositioningService.java org/openbmap/activities/Selective ScrollViewPager.java
				a/a/a/o.java org/openbmap/c/n.java org/openbmap/c/a.java org/openbmap/activities/SettingsA ctivity.java org/openbmap/c/j.java
				org/openbmap/db/c.java org/openbmap/activities/x.java org/openbmap/db/RadioBeaconC ontentProvider.java org/openbmap/utils/VerticalLabel View.java

NO	ISSUE	SEVERITY	STANDARDS	org/openbmap/utils/ab.java org/openbmap/activities/ay.java org/openbmap/activities/b.java
				org/openbmap/db/b.java com/a/a/cq.java org/openbmap/services/positionin g/a/a.java org/openbmap/c/i.java org/openbmap/utils/w.java org/openbmap/services/wireless/ WirelessLoggerService.java org/openbmap/c/e.java org/openbmap/activities/StatsActi vity.java
2	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/utils/n.java org/openbmap/utils/am.java org/openbmap/utils/ar.java org/openbmap/activities/aw.java org/openbmap/db/c.java org/openbmap/utils/ab.java org/openbmap/activities/b.java org/openbmap/db/b.java org/openbmap/utils/w.java org/openbmap/services/wireless/ WirelessLoggerService.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	org/openbmap/utils/ao.java org/openbmap/utils/ar.java org/openbmap/activities/WifiDetai lsActivity.java org/openbmap/db/c.java org/openbmap/db/RadioBeaconC ontentProvider.java org/openbmap/db/b.java org/openbmap/services/wireless/ WirelessLoggerService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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
5	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
6	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
7	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/h.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

Q 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

DOMAIN	STATUS	GEOLOCATION
barcelonabusturistic.cat	ok	IP: 52.48.10.217 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
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
code.google.com	ok	IP: 142.250.179.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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

Т

DOMAIN	STATUS	GEOLOCATION
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
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
www.radiocells.org	ok	IP: 94.79.179.26 Country: Germany Region: Rheinland-Pfalz City: Kerpen Latitude: 50.309669 Longitude: 6.729780 View: Google Map

Т



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

HARDCODED SECRETS

POSSIBLE SECRETS
"prefs_credentials_password" : "Password"
"prefs_credentials_user" : "Login"
"sessions" : "Sessions"
"prefs_credentials" : "Credentials"
"prefs_credentials_password_summary" : ""
"prefs_credentials_password" : "Adgangskode"
"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?"

POSSIBLE SECRETS
"prefs_auto_delete_sessions_title" : "古いセッションをクリーンアップ"
"prefs_credentials_password" : "パスワード"
"prefs_credentials_user" : "ログイン"
"question_delete_session" : "セッションを削除しますか?"
"question_enter_user" : "今、ユーザー名とパスワードを入力しますか?"
"session_already_uploaded" : "セッションはすでにアップロード済です"
"session_uploaded" : "セッションをアップロードしました"
"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!"
"prefs_credentials" : "資格情報"
"prefs_credentials_password" : "Passwort"
"prefs_credentials_user" : "User"
"sessions" : "Sitzungen"
"prefs_credentials" : "Login-Daten"
"prefs_credentials_password" : "Wachtwoord"



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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.