MOBSF

ANDROID STATIC ANALYSIS REPORT

Network Monitor (1.32.0)

File Name:	installer168.apk
Package Name:	ca.rmen.android.networkmonitor
Scan Date:	May 31, 2022, 4:58 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	8	1	1	1

FILE INFORMATION

File Name: installer168.apk
Size: 2.31MB
MD5: b36891183cd6ed2342e5a2f82e82af94
SHA1: 1d6995eadcdcaadf6b4e0e4201814fe0b5e2226e
SHA256: 9c250984ba9c29442e3f64093fb6e1ff58a21f18bc01e012e2ec5bb0954c9368

APP INFORMATION

App Name: Network Monitor
Package Name: ca.rmen.android.networkmonitor
Main Activity: ca.rmen.android.networkmonitor.app.main.MainActivity
Target SDK: 28
Min SDK: 14
Max SDK:
Android Version Name: 1.32.0
Android Version Code: 13200

APP COMPONENTS

Activities: 13
Services: 3
Receivers: 1
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
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: 2015-04-27 10:24:19+00:00
Valid To: 2042-09-12 10:24:19+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x325195db
Hash Algorithm: sha256
md5: d3447b2243eb06911d09ee5a5ad2bdc6
sha1: facae42b334e27976ad67958269acaf22270abba
sha256: 310bdad3832d2d4ab9c8a3eb3b98df579adc702b8d3ebb8ceba22fd56fcc204e
sha512: 7f1f17c9e6dcf98dc148fb4f9bf69356f9a3ba3d366858e27bf5a8eb1e63fab7bff0a4c5e583d268ce5b6b1ca4dec387ba01c2cfa9dabf490029c4884e6f34ca

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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
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
classes.dex	FINDINGS: DETAILS Compiler: r8

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 (ca.rmen.android.networkmonitor.app.savetostorage.SaveToStorageActivity) 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	Broadcast Receiver (ca.rmen.android.networkmonitor.app.service.BootReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver 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 Broadcast Receiver is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ca/rmen/android/networkmonitor/app/service/datasources/ConnectionTesterDataSource.java ca/rmen/android/networkmonitor/app/dialog/ConfirmDialogFragment.java ca/rmen/android/networkmonitor/app/dialog/ChoiceDialogFragment.java ca/rmen/android/networkmonitor/app/speedtest/SpeedTestUpload.java ca/rmen/android/networkmonitor/util/IoUtil.java ca/rmen/android/networkmonitor/app/main/WarningDialogFragment.java

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	ca/rmen/android/networkmonitor/app/dbops/backend/export/HTMLExport.java ca/rmen/android/networkmonitor/app/dbops/backend/export/TableFileExport.java ca/rmen/android/networkmonitor/app/about/AboutActivity.java org/greenrobot/eventbus/BackgroundPoster.java ca/rmen/android/networkmonitor/app/dbops/backend/imp0rt/DBImport.java ca/rmen/android/networkmonitor/app/service/NetMonService.java ca/rmen/android/networkmonitor/app/service/datasources/NetMonDataSources.java ca/rmen/android/networkmonitor/app/dbops/backend/export/kml/KMLExport.java ca/rmen/android/networkmonitor/util/AndroidConstantsUtil.java ca/rmen/android/networkmonitor/app/service/datasources/NetworkInterfaceDataSource.java jxl/common/log/SimpleLogger.java ca/rmen/android/networkmonitor/provider/NetMonDatabase.java ca/rmen/android/networkmonitor/util/NetMonSignalStrength.java ca/rmen/android/networkmonitor/app/prefs/SettingsExportImport.java ca/rmen/android/networkmonitor/app/email/ReportEmailer.java ca/rmen/android/networkmonitor/app/dbops/backend/export/ExcelExport.java org/greenrobot/eventbus/EventBus.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	ca/rmen/android/networkmonitor/app/prefs/NetMonPreferences.java ca/rmen/android/networkmonitor/app/service/NetMonService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	jxl/write/biff/FileDataOutput.java
4	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	ca/rmen/android/networkmonitor/util/FileUtil.java ca/rmen/android/networkmonitor/app/speedtest/SpeedTestPreferencesActivity.java
5	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	ca/rmen/android/networkmonitor/provider/NetMonDatabase.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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_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.
11	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-MD5'] .
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
rmen.ca	ok	**IP:** 213.186.33.18 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
earth.google.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
goo.gl	ok	**IP:** 216.58.214.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
psdev.de	ok	**IP:** 49.12.32.214 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.linkedin.com	ok	**IP:** 13.107.42.14 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
bitaether.net	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
jraf.org	ok	**IP:** 158.69.221.169 **Country:** Canada **Region:** Quebec **City:** Beauharnois **Latitude:** 45.316780 **Longitude:** -73.865898 **View:** Google Map

EMAILS

EMAIL	FILE
c@rmen.ca bod@jraf.org user@domain.com user@gmail.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"pref_summary_email_user" : "%s"
"pref_summary_speed_test_upload_user" : "%s"
"pref_summary_email_user" : "%s"

POSSIBLE SECRETS
"pref_summary_speed_test_upload_user" : "%s"
"pref_summary_email_user" : "%s"
"pref_summary_speed_test_upload_user" : "%s"

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.