ANDROID STATIC ANALYSIS REPORT

Orange Money (3.1.4)

File Name:	com.orange.orangemoneycameroun_22640.apk
Package Name:	com.orange.orangemoneycameroun
Average CVSS Score:	6.9
App Security Score:	70/100 (MEDIUM RISK)

FILE INFORMATION

File Name: com.orange.orangemoneycameroun_22640.apk
Size: 3.81MB
MD5: b78c0e59d595df3f52420f807fd63c54
SHA1: bca149a124cd384d7f672464bd4f6aeadf5bd308
SHA256: fba9282fa00b104e303779977379f3b94c6d349677384865d3aea827474c73d8

APP INFORMATION

App Name: Orange Money
Package Name: com.orange.orangemoneycameroun
Main Activity: com.orange.orangemoneylib.activity.SplashScreenSubscriber
Target SDK: 25
Min SDK: 16
Max SDK:
Android Version Name: 3.1.4
Android Version Code: 22640

APP COMPONENTS

Activities: 47
Services: 1
Receivers: 0
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=London, L=London, O=Orange, OU=Orange , CN=Orange_Android_Certificate
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-06-30 09:31:21+00:00
Valid To: 2036-11-15 09:31:21+00:00
Issuer: C=UK, ST=London, L=London, O=Orange, OU=Orange , CN=Orange_Android_Certificate
Serial Number: 0x4a49db69
Hash Algorithm: sha1
md5: f351ae8ce0fe457eaaf708042ce2c909
sha1: 513c0ea5fc5dea245c63ec453269e912665dd118
sha256: b67affcda89e3193b1595036d7c6cdbe22be5ca24c9f6cf93fc6b48f91d7310d
sha512:
3b966a10dc81aadd50e1536640d84071706adabfb36cae8ae7c07f0aa50bd0e49fc976fcb5e6ff2887b5119b9d3614ee8e10796bc4e0a8bd8113d866433ab8b6

PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 14fec33b0cf9e36b47a64871038e3396f333b19052431a0b4f8b6ce4e289ebcf

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.INTERNET	dangerous	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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
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.DOWNLOAD_WITHOUT_NOTIFICATION	dangerous	Unknown permission from android reference	Unknown permission from android reference
		Unknown	Unknown permission from android

com.google.android.providers.gsf.permission.READ_GSERVICES	dangerous	permission from android reference	reference
com.orange.myorange.permission.MAPS_RECEIVE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: SIM operator check network operator name check FINDINGS: Compiler — DETAILS: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup=true]	medium	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.
Activity (com.orange.orangemoneylib.activity.ExternalSplashScreen) is not Protected. An intent-filter exists.	high	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.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			defpackage/aa.java defpackage/az.java defpackage/ai.java defpackage/am.java defpackage/r.java defpackage/bk.java defpackage/bj.java defpackage/ah.java defpackage/at.java defpackage/d.java defpackage/bg.java defpackage/al.java defpackage/x.java

The App logs information. Sensitive information should	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File	defpackage/ad.java defpackage/bv.java defpackage/ac.java defpackage/bh.java defpackage/aj.java defpackage/bu.java defpackage/ax.java defpackage/ag.java defpackage/g.java defpackage/bi.java defpackage/bt.java defpackage/ab.java defpackage/v.java defpackage/j.java defpackage/au.java defpackage/ba.java defpackage/ae.java com/orange/orangemoneylib/backend/beans/Grade.java com/orange/orangemoneylib/backend/beans/Transaction.java com/orange/orangemoneylib/backend/beans/Pin.java com/orange/orangemoneylib/backend/beans/StoreList.java com/orange/orangemoneylib/backend/beans/SectionList.java com/orange/orangemoneylib/activity/AboutActivity.java com/orange/orangemoneylib/activity/ErrorActivity.java com/orange/orangemoneylib/activity/PopUpCallMap.java com/orange/orangemoneylib/activity/SubscriptionFormActivity.java com/orange/orangemoneylib/activity/AllStoresActivity.java com/orange/orangemoneylib/activity/PopUpIntTransf.java com/orange/orangemoneylib/activity/SubscriptionMSISDNActivity.java com/orange/orangemoneylib/activity/SplashScreenSubscriber.java com/orange/orangemoneylib/activity/ErrorUSSDCancel.java com/orange/orangemoneylib/activity/MenuActivity.java com/orange/orangemoneylib/activity/SubscriptionStatusScreenActivity.java com/orange/orangemoneylib/activity/StartTransferIrtMainActivity.java com/orange/orangemoneylib/activity/PopUpCallCustomerCare.java com/orange/orangemoneylib/activity/TransactionSummaryActivity.java com/orange/orangemoneylib/activity/OMApplication.java com/orange/orangemoneylib/activity/FormActivity.java com/orange/orangemoneylib/activity/ExternalSplashScreen.java com/orange/orangemoneylib/activity/ErrorUSSDParameter.java com/orange/orangemoneylib/activity/a.java

never be logged.		**OWASP MASVS:** MSTG-STORAGE-3	com/orange/orangemoneylib/activity/JSPinPadActivity.java com/orange/orangemoneylib/activity/StoreDetailActivity.java com/orange/orangemoneylib/activity/PinPadActivity.java com/orange/orangemoneylib/activity/StoreAroundMeActivity.java com/orange/orangemoneylib/activity/WebViewActivity.java com/orange/orangemoneylib/activity/StoreMapV2Activity.java com/orange/orangemoneylib/activity/SubscriptionPinPadActivity.java com/orange/orangemoneylib/activity/AnalyticsSettingsActivity.java com/orange/orangemoneylib/activity/PopUpCallParameter.java com/orange/orangemoneylib/activity/SplashScreenRetailer.java com/orange/orangemoneylib/activity/MainMenu.java com/orange/orangemoneylib/classicqueries/InternationalTransfertInitActivity.java com/orange/orangemoneylib/classicqueries/GenericTransactionQueryActivity.java com/orange/orangemoneylib/classicqueries/Last5transactionsActivity.java com/orange/orangemoneylib/classicqueries/OTPActivity.java com/orange/orangemoneylib/classicqueries/TransferIRTMainQueryActivity.java com/orange/orangemoneylib/classicqueries/ChangeLangToggleActivity.java com/orange/orangemoneylib/classicqueries/BalanceActivity.java com/orange/orangemoneylib/classicqueries/BalanceDoubleActivity.java com/orange/orangemoneylib/classicqueries/a.java com/orange/orangemoneylib/classicqueries/TransferIRTMainConfirmActivity.java com/orange/orangemoneylib/classicqueries/ChangePinActivity.java com/orange/orangemoneylib/classicqueries/TransferIRTMainActivity.java com/orange/orangemoneylib/classicqueries/ChangeLangActivity.java com/orange/orangemoneylib/utils/p.java com/orange/orangemoneylib/utils/l.java com/orange/orangemoneylib/utils/c.java com/orange/orangemoneylib/utils/o.java com/orange/orangemoneylib/utils/e.java com/orange/orangemoneylib/utils/n.java com/orange/orangemoneylib/utils/k.jav

			a com/orange/orangemoneylib/utils/a.java a com/orange/orangemoneylib/utils/m.java com/orange/orangemoneylib/utils/g.java a com/orange/orangemoneylib/utils/q.java a com/orange/orangemoneylib/utils/f.java a
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.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	defpackage/af.java
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-295 - Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	defpackage/x.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
omapp-localservices.kermit.orange-labs.fr	good	No Geolocation information available.
schemas.android.com	good	No Geolocation information available.
webapps.elibel.tm.fr	good	No Geolocation information available.

URLS

URL	FILE
http://omapp-localservices.kermit.orange-labs.fr/app1/getInternationalGradeFull.html http://omapp-localservices.kermit.orange-labs.fr/app1/getDoubleBalanceFull.html	defpackage/ad.java
http://schemas.android.com/apk/res/android	defpackage/e.java
file:///android_asset/	com/orange/orangemoneylib/activity/LegalsActivity.java
http://subscription http://selected_bank_account http://selected_bank_name http://selected_bank_acount	

http://map_app_name http://transfer_amount http://fee_amount http://wholesaler_name http://webapps.elibel.tm.fr/OMApp http://selected_bank	Android String Resource

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.9 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.