MOBSF

ANDROID STATIC ANALYSIS REPORT

MTN MoMo (1.0.1)

File Name:	mtn-momo_1.0.1.apk
Package Name:	com.consumerug
Average CVSS Score:	5.3
App Security Score:	25/100 (HIGH RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: mtn-momo_1.0.1.apk
Size: 6.74MB
MD5: 4c21a20b8ef87d4282b812090831cfda
SHA1: 2fc56b233227a8c483d885aed3c4116858aecd2d
SHA256: d7c25976223d526bfe9d5cef6021e76cf794c25e1914f613e9ba054c68bd7d54

APP INFORMATION

App Name: MTN MoMo
Package Name: com.consumerug
Main Activity: com.comviva.webaxn.ui.WebAxnActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 1.0.1
Android Version Code: 10907

APP COMPONENTS

Activities: 11
Services: 6
Receivers: 5
Providers: 1
Exported Activities: 0
Exported Services: 1
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=91, ST=Karnataka, L=Bangalore, O=Comviva, OU=MLS, CN=Anup Raghvan
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-17 12:42:05+00:00
Valid To: 2037-04-11 12:42:05+00:00
Issuer: C=91, ST=Karnataka, L=Bangalore, O=Comviva, OU=MLS, CN=Anup Raghvan
Serial Number: 0x4f8d651d
Hash Algorithm: sha1
md5: 26b0fb1e7830f33152ad05a01418bf96
sha1: c0b18dfbc0425f05a6b02602b308466f02003482
sha256: 1d3cdcd45229dac4aa6daadf5859967a2035823d1450556c210a5ea2d33b6dac
sha512:
cd18b9ca75d1012d6976f6c3123fc04f0b3ea736399f30f8dcf016c77e920d27e51869cb19d6b295ae0addcbebabd7258c4a6083d523acc9e806b0d9fb0a3dba

PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 9216875bc691956816e2f75d0d2c2e1e9326962de4dd04b40995abb32cc6fee0

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.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead
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.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.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.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.

android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check subscriber ID check FINDINGS: Compiler — DETAILS: dx

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.comviva.webaxn.ui.WebAxnActivity	Schemes: @string/schema://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
Launch Mode of Activity (com.comviva.webaxn.ui.WebAxnActivity) 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.
Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	defpackage/eo.java defpackage/p.java defpackage/s.java defpackage/ct.java defpackage/sg.java defpackage/cd.java defpackage/ce.java defpackage/rx.java defpackage/cm.java defpackage/cx.java defpackage/lv.java defpackage/io.java defpackage/at.java defpackage/si.java defpackage/lx.java defpackage/so.java defpackage/rv.java defpackage/av.java defpackage/ru.java defpackage/fb.java defpackage/di.java defpackage/dr.java defpackage/ng.java defpackage/sx.java defpackage/ax.java defpackage/cc.java defpackage/da.java defpackage/cf.java defpackage/lw.java defpackage/gn.java defpackage/rz.java defpackage/gm.java defpackage/sc.java defpackage/by.java defpackage/rw.java defpackage/jg.java defpackage/qc.java defpackage/sd.java defpackage/is.java

			defpackage/au.java defpackage/tb.java defpackage/bx.java defpackage/cq.java defpackage/cw.java com/comviva/webaxn/ui/l.java com/comviva/webaxn/utils/bb.java com/comviva/webaxn/utils/ax.java com/comviva/webaxn/utils/bs.java com/viewpagerindicator/a.java com/airbnb/lottie/l.java com/airbnb/lottie/d.java com/airbnb/lottie/c.java com/airbnb/lottie/e.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/f.java com/triggertrap/seekarc/SeekArc.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	defpackage/p.java defpackage/tn.java defpackage/ju.java defpackage/jr.java defpackage/dz.java defpackage/cm.java defpackage/jd.java defpackage/jm.java defpackage/io.java defpackage/Cdo.java defpackage/jh.java defpackage/js.java defpackage/iy.java defpackage/gv.java defpackage/iw.java defpackage/jf.java defpackage/jt.java defpackage/iz.java defpackage/tm.java defpackage/wp.java defpackage/ed.java defpackage/wo.java defpackage/jb.java defpackage/it.java defpackage/du.java defpackage/jq.java defpackage/ci.java defpackage/iv.java defpackage/dw.java defpackage/jp.java defpackage/eg.java defpackage/iq.java defpackage/im.java defpackage/br.java defpackage/jl.java defpackage/je.java defpackage/gp.java defpackage/ee.java defpackage/cj.java defpackage/jg.java defpackage/jn.java

			defpackage/is.java defpackage/in.java defpackage/q.java defpackage/gr.java defpackage/jc.java defpackage/il.java com/comviva/webaxn/utils/ax.java
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/ks.java defpackage/se.java
App creates temp file. Sensitive information should never be written into a temp file.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/ax.java com/theartofdev/edmodo/cropper/c.java com/theartofdev/edmodo/cropper/CropImageActivity.java
IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor OWASP MASVS: MSTG-CODE-2	defpackage/ln.java com/comviva/webaxn/ui/aw.java com/comviva/webaxn/ui/WebAxnActivity.java com/comviva/webaxn/utils/DataSyncService.java com/comviva/webaxn/utils/ak.java com/comviva/webaxn/transport/a.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	defpackage/sd.java com/comviva/webaxn/utils/bj.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/comviva/webaxn/utils/l.java com/comviva/webaxn/utils/bj.java com/comviva/webaxn/utils/bq.java com/comviva/webaxn/utils/ax.java
This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	com/comviva/webaxn/utils/bq.java
SHA-1 is a weak hash known to have hash collisions.	high	CVSS V2: 5.9 (medium) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/comviva/webaxn/utils/ax.java com/comviva/webaxn/utils/bc.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	good	**IP:** 108.177.119.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
mymtnapp2.mtn.co.ug	good	**IP:** 212.88.125.200 **Country:** Uganda **Region:** Kampala **City:** Kampala **Latitude:** 0.31628 **Longitude:** 32.582191 **View:** Google Map
pagead2.googlesyndication.com	good	**IP:** 172.217.218.155 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
maps.google.com	good	**IP:** 108.177.119.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://www.googleapis.com/auth/fitness.activity.read https://www.googleapis.com/auth/fitness.activity.write https://www.googleapis.com/auth/fitness.location.read https://www.googleapis.com/auth/fitness.location.write https://www.googleapis.com/auth/fitness.body.read https://www.googleapis.com/auth/fitness.body.write https://www.googleapis.com/auth/fitness.nutrition.read https://www.googleapis.com/auth/fitness.nutrition.write	defpackage/ns.java
http://schemas.android.com/apk/res/android	defpackage/cr.java
https://www.google.	defpackage/sw.java
https://maps.google. https://www.google. https://books.google.	defpackage/so.java

https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	defpackage/lw.java
https://www.googleapis.com/auth/fitness.activity.read https://www.googleapis.com/auth/fitness.activity.write https://www.googleapis.com/auth/fitness.location.read https://www.googleapis.com/auth/fitness.location.write https://www.googleapis.com/auth/fitness.body.read https://www.googleapis.com/auth/fitness.body.write https://www.googleapis.com/auth/fitness.nutrition.read https://www.googleapis.com/auth/fitness.nutrition.write https://www.googleapis.com/auth/fitness.blood_pressure.read https://www.googleapis.com/auth/fitness.blood_pressure.write https://www.googleapis.com/auth/fitness.blood_glucose.read https://www.googleapis.com/auth/fitness.blood_glucose.write https://www.googleapis.com/auth/fitness.oxygen_saturation.read https://www.googleapis.com/auth/fitness.oxygen_saturation.write https://www.googleapis.com/auth/fitness.body_temperature.read https://www.googleapis.com/auth/fitness.body_temperature.write https://www.googleapis.com/auth/fitness.reproductive_health.read https://www.googleapis.com/auth/fitness.reproductive_health.write	defpackage/oc.java
file:///android_asset/map/	defpackage/ln.java
https://www.googleapis.com/books/v1/volumes?q=isbn: http://www.google.	defpackage/sv.java
https://mymtnapp2.mtn.co.ug/webaxn/webaxn?group=consumerapp&platform=android	defpackage/kr.java
http://maps.google.com/maps?saddr=	com/comviva/webaxn/utils/bj.java

TRACKERS

TRACKER	URL
Google Analytics	https://reports.exodus-privacy.eu.org/trackers/48

PLAYSTORE INFORMATION

Title: MTN MoMo

Score: 3.95 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Finance **Play Store URL:** com.consumerug

Developer Details: MTN, MTN, None, http://www.mtn.com, webaxn_support@mahindracomviva.com,

Release Date: Nov 1, 2019 **Privacy Policy:** Privacy link

Description:

Welcome to the world of services to suit everyone's needs. With MTNMoMo you can topup airtime, purchase bundles pay your bills and much more. It's everything you need, all in one place. Manage your mobile money the easy way with MTNMoMo. MTNMoMo gives subscribers greater control of their own mobile money services so that they can access MTN services and solve issues without having to contact company representatives.

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.

© 2020 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.