MOBSF

ANDROID STATIC ANALYSIS REPORT

Nexttel Possa (1.4.2)

File Name:	nexttel-possa_1.4.2.apk
Package Name:	com.nexttel.possa
Average CVSS Score:	6.7
App Security Score:	60/100 (MEDIUM RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: nexttel-possa_1.4.2.apk
Size: 5.94MB
MD5: 1e0a9c56163e9f0a61e9262ce668fe59
SHA1: ce47430321e2be36fbc8e6fc3952052529438393
SHA256: bddb55e317c6149263226b74c875583daf15cd33dcc90946e42a8697ec700245

APP INFORMATION

App Name: Nexttel Possa
Package Name: com.nexttel.possa
Main Activity: com.nexttel.possa.SplashScreenActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 1.4.2
Android Version Code: 22

APP COMPONENTS

Activities: 9
Services: 6
Receivers: 3
Providers: 1
Exported Activities: 0
Exported Services: 4
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=Nexttel
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-10-21 09:21:53+00:00
Valid To: 2041-10-15 09:21:53+00:00
Issuer: O=Nexttel
Serial Number: 0x7de8bd86
Hash Algorithm: sha256
md5: c5a03a321b1bd1100eb7a3f109e28414
sha1: 6b9a2e610aab934683c749150691f3e7951b9859
sha256: 3f64a0112cc01d05c3c59b3b2fa0aa2b753301661e702ff8278c7da9ce4a6cbf

sha512:
2aa874075fdbf6535bdb0112718d0c00fc5dcfe0cd1c0f2c97535cacdfc8706dc54e7c0d50b67e4d090786ceed83873d7e75fd2c435faffbdb1089fb502ba2ca

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9a141bf1cb51fd18320aad2821dd20b077f662b70b8ab9b19fd9371b36ccb77e

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.creova.mpay.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
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.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.nexttel.possa.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.

APKID ANALYSIS

FILE	DETAILS
classes.dex	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.
Service (com.nexttel.possa.services.MyFirebaseMessagingService) is not Protected. [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.
Service (com.nexttel.possa.services.MyFirebaseInstanceIDService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	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. 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.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	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. 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.

Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [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.

</> 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	com/nexttel/possa/Ag_NewClientFragment.java com/nexttel/possa/FeedBack.java com/nexttel/possa/InternetRechargeFragment1.java com/nexttel/possa/Transaction_detail_Fragment.java com/nexttel/possa/ENEOFragment3.java com/nexttel/possa/tabActivity.java com/nexttel/possa/SplashScreenActivity.java com/nexttel/possa/AirTimeFragment.java com/nexttel/possa/MainActivity.java com/nexttel/possa/ChangeFirstPasswordActvity.java com/nexttel/possa/ENEOFragmentPrepayed.java com/nexttel/possa/ChangeFirstPassword.java com/nexttel/possa/HistoriqueFragment.java com/nexttel/possa/InternetRechargeFragment4.java com/nexttel/possa/InternetRechargeFragment3.java com/nexttel/possa/MyWallet.java com/nexttel/possa/MyPossaFragment.java com/nexttel/possa/ENEOFragment2.java com/nexttel/possa/Helper/RequetHttp.java com/nexttel/possa/Helper/Constants.java com/nexttel/possa/Helper/KeyboardListener.java com/nexttel/possa/Helper/SwissKnife.java com/nexttel/possa/services/MyFirebaseMessagingService.java com/nexttel/possa/services/MyFirebaseInstanceIDService.java com/nexttel/possa/adapters/MyAdapter.java com/nexttel/possa/utils/NetworkChangeReceiver.java
		CVSS V2: 7.5 (high)	

The App uses an insecure Random Number Generator.	high	**CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	com/nexttel/possa/Transaction_detail_Fragment.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	com/nexttel/possa/Helper/RequetHttp.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	com/nexttel/possa/Helper/MD5.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
nexttel-possa.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
possa.mgw.creova.com	good	**IP:** 163.172.225.75 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.3488 **View:** Google Map
pmgw.nexttel.cm	good	No Geolocation information available.
192.168.1.70	good	**IP:** 192.168.1.70 **Country:** - **Region:** - **City:** - **Latitude:** 0.0 **Longitude:** 0.0 **View:** Google Map
nexttel.mgw.creova.com	good	**IP:** 163.172.225.75 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.3488 **View:** Google Map
		IP: 163.172.225.75 **Country:** France

possa.notification.creova.com	good	**Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.3488 **View:** Google Map
www.nexttel.cm	good	**IP:** 41.244.254.22 **Country:** Cameroon **Region:** Centre **City:** Yaounde **Latitude:** 3.86667 **Longitude:** 11.51667 **View:** Google Map

URLS

URL	FILE
http://possa.mgw.creova.com:8010/creova.php	com/nexttel/possa/InternetRechargeFragment1.java
http://www.nexttel.cm/	com/nexttel/possa/HelpFragment.java
http://www.nexttel.cm/	com/nexttel/possa/HelpsActivity.java
http://possa.mgw.creova.com:8010/creova.php http://192.168.1.70:8888/MintRoute-Server/mintroute.php	com/nexttel/possa/Helper/RequetHttp.java
http://possa.notification.creova.com:8010/newRegister.php http://pmgw.nexttel.cm:8010/creova.php http://possa.mgw.creova.com:8010/creova.php http://nexttel.mgw.creova.com:8010/creova.php	com/nexttel/possa/Helper/Constants.java
https://nexttel-possa.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://nexttel-possa.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: Nexttel Possa

Score: 3.9545455 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Finance **Play Store URL:** com.nexttel.possa

Developer Details: Creova, Creova, None, http://www.creova.com, dev@creova.com,

Release Date: Nov 14, 2017 **Privacy Policy:** Privacy link

Description:

Possa est le nouveau service de neXttel qui vous permet de recevoir et d'envoyer de l'argent à petit coût partout au Cameroun. Avec neXttel Possa, envoyez de l'argent à vos proches, payez vos factures, rechargez votre téléphone, en tout rapidité, simplicité et sécurité.

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.