APP SCORES

Security Score **49/100**

Trackers Detection **1/432**

FILE INFORMATION

File Name KMBL.apk

Size 20.15MB

MD5 0b41adb1df7c2ce11d07e521787277ce

SHA1 72706f21806d661cde2fe98fe8f39afaa8397b4c

SHA256 47c2157e8b26da7d400d073af8413c955e401cb77196ae0d5199808591094575

APP INFORMATION

App Name KMBL

Package Name com.KMBL.retail

Main Activity com.temenos.edgehybrid.EdgeActivity

Target SDK 32 Min SDK 22 Max SDK

Android Version Name 2.0.4 Android Version Code 20232

PLAYSTORE INFORMATION

Title Khushhali

Score 2.4285715 Installs 100,000+ Price 0 Android Version Support Category Finance Play Store URL com.KMBL.retail

Developer Khushhali Microfinance Bank Ltd., Developer ID Khushhali+Microfinance+Bank+Ltd.

Developer Address Plot 55-C, 7th floor, Ufone Tower, Blue Area Islamabad Khushhali Microfinance Bank, Corporate Office.

Developer Website https://www.khushhalibank.com.pk/

Developer Email complaints@kb.com.pk

Release Date Dec 2, 2019 Privacy Policy Privacy link

Description

Khushhali Microfinance Bank stays true to its tradition of bringing you the most cutting edge banking and financial services that enable you to do more, and brings a whole new world of convenience and connectivity with Khushhali mobile app.

Khushhali mobile app enables you to have complete control on your bank account with the following features:

1. Interbank funds transfer
2. Funds transfer
3. Bill payments
4. Mobile balance Top-up
5. Balance inquiry
6. Mini statement
7. Banker Cheque request
8. Cheque book request

Khushhali mobile app lets you stay connected to your bank account in real-time* so you manage your finances from anywhere, at any time.

GET STARTED:

• If you are already have an active internet banking account, simply download the app, log in using your Internet Banking User ID, and password, and you’re ready to go!
• If you haven’t signed up to Internet Banking Service, register through the app and then call Khushhali Bank Helpline on (051) 111-047-047 to activate your internet banking account.

SUPPORT:

Having general app issues? Visit our in-app Help section or easily get in touch with a friendly Khushhali Bank representative by dialing (051)111-047-047.

Khushhali Microfinance Bank does not charge fees to download or use the Khushhali Mobile app or internet banking services; however, message and data rates may apply. Contact your mobile provider for information about any fees that might be imposed. Some features are only available for eligible customers and accounts only. Any time you review your balance, keep

in mind it may not reflect all transactions including recent debit card transactions or cheques you have written.

For more information, refer to the Mobile Banking Terms/Service Agreement provided to you upon signup.

For more information related to customer support:
- 24/7 Helpline: 111-047-047
- Email: complaints@kb.com.pk
- Desktop view: https://login.khushhalibank.com.pk/
- Corporate Website: https://khushhalibank.com.pk/

4

ACTIVITIES

View

8

SERVICES

View

4

RECEIVERS

View

3

PROVIDERS

View

Exported Activities
0

Exported Services
1

Exported
Receivers
2

Exported
Providers
0

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-02 05:54:55+00:00
Valid To: 2049-12-02 05:54:55+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe13db3c27a49f6b323c900c01a05d7e5764d4c11
Hash Algorithm: sha256
md5: 23820963651ea7894d27e0b53be0a54e
sha1: 528835523380d55bb4986d34135bcbe5e7a2c010
sha256: 6f7d108c380428cba67beef5fed45eb439f97d2c4f4721394062bb371258ea43
sha512:
417479ab14ddec33a7a240efd923b220783eaf42ca2aafa9f9ff05ecc4bd944ffe06c446804ca2e3c97ba9bc5b0e487a05b63145697ad0383b13a3aaf83
eb543
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 605c981ccb48567f7970c622b133821792c2813c3473cdf23b86f75d65d623ff
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

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

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.	

Showing 1 to 10 of 13 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	

API	FILES
Crypto	
Execute OS Command	
Get System Service	
HTTP Connection	
HTTPS Connection	
Inter Process Communication	
Java Reflection	

Showing 1 to 10 of 17 entries

Previous 1 2 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	0	0	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

Showing 1 to 1 of 1 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	3	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
3	**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]	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. 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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
4	**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]	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. 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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
5	**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]	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. 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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			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.	

Showing 1 to 5 of 5 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	5	1	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
2	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	i1/a.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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	u0/d0.java u0/e0.java u0/z.java	
4	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1	j2/a.java k2/b.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
5	This App may request root (Super User) privileges.	warning	**CWE:** CWE-250: Execution with Unnecessary Privileges **OWASP MASVS:** MSTG-RESILIENCE-1	j2/a.java k2/a.java	
6	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	b2/b.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
7	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	b2/c.java	
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4	i2/i.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
9	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	**CWE:** CWE-295: Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	com/temenos/edgehybrid/components/EdgeWebViewClientHelper.java	

Showing 1 to 9 of 9 entries

Previous 1 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table								

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check possible ro.secure check
Compiler	dx

Showing 1 to 3 of 3 entries

Previous 1 Next

Showing 1 to 1 of 1 entries

Previous 1 Next

QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

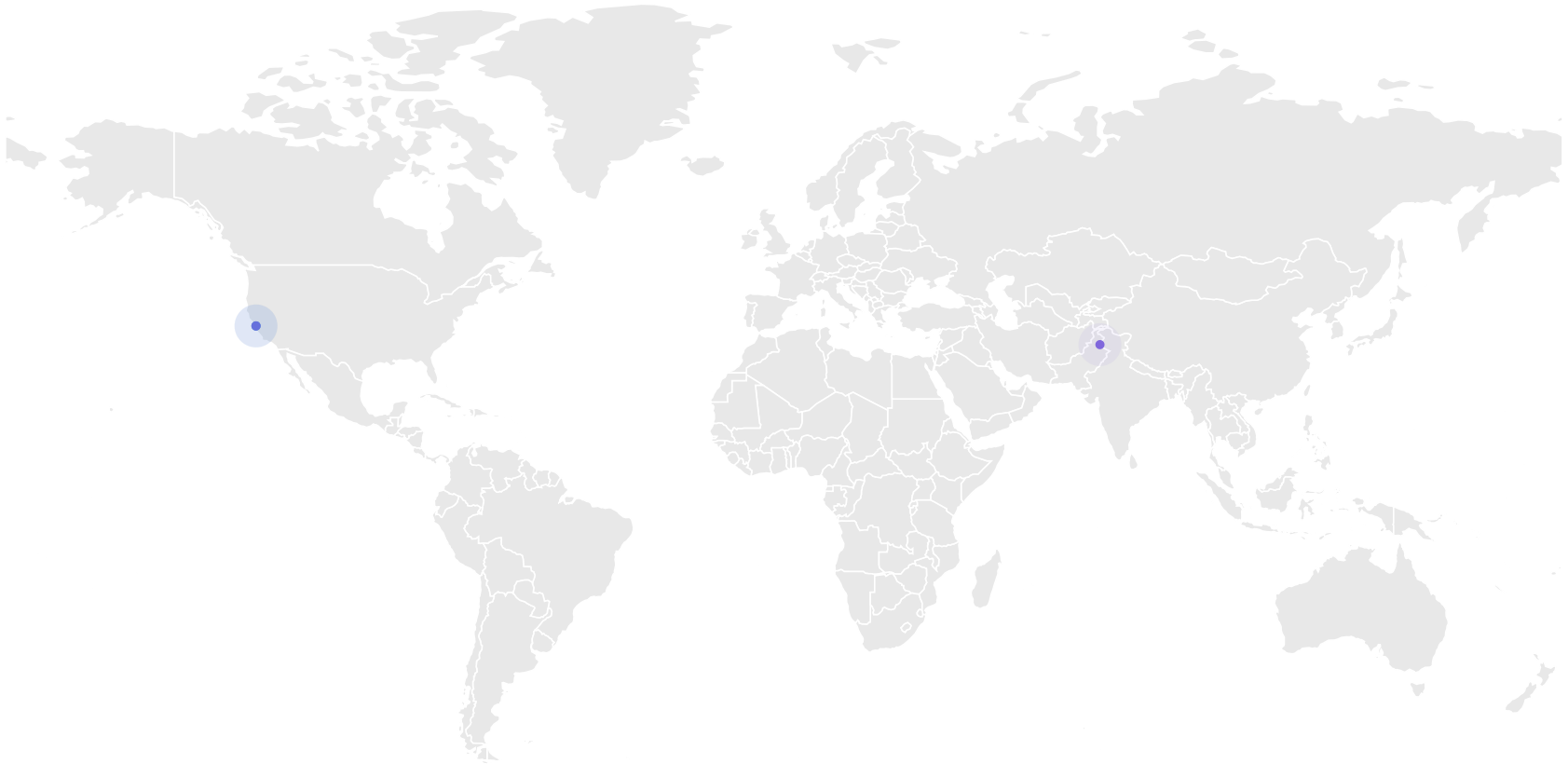
Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	9/24	Other Common Permissions	4/4
android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.GET_ACCOUNTS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK		android.permission.ACCESS_LOCATION_EXTRA_COMMANDS, android.permission.WRITE_CONTACTS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVIC	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 74.125.71.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
moblogin.khushhalibank.com.pk	ok	**IP:** 202.125.155.72 **Country:** Pakistan **Region:** Punjab **City:** Rawalpindi **Latitude:** 33.600700 **Longitude:** 73.067902 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.181.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.181.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

Showing 1 to 5 of 5 entries

Previous 1 Next

URLS

Search:

URL	FILE
file:///android_asset/common_jailbreakerror.html file:///android_asset/common_offlineerror.html javascript:try file:///android_asset/ file:///android_asset/common_forceupdateerror.html file:///android_asset/common_sslerror.html	com/temenos/edgehybrid/components/EdgeWebViewClientHelper.java
file:///android_asset/htmlerrorpages/checkforupdateserrorpage.html http://play.google.com/store/apps/details?id=	com/temenos/edgehybrid/EdgeActivity.java
http://schemas.android.com/apk/res/android	n/i.java
https://%s/%s/%s	c2/c.java
https://accounts.google.com/o/oauth2/revoke?token=	d1/e.java

URL	FILE
https://moblogin.khushhalibank.com.pk:5055/retail/mobileupdate https://moblogin.khushhalibank.com.pk:5055/retail/servletcontroller	g2/a.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	y0/b.java

Showing 1 to 7 of 7 entries

Previous 1 Next

FIREBASE DATABASE

EMAILS

TRACKERS

Search:

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

Showing 1 to 1 of 1 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

STRINGS

From APK Resource

▶ Show all **3192** strings

From Code

▶ Show all **5328** strings

From Shared Objects

ACTIVITIES

▼ Showing all **4** activities

com.temenos.edgehybrid.EdgeActivity
com.temenos.edgehybrid.AppPreferences
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
com.google.android.gms.common.api.GoogleApiActivity

SERVICES

▼ Showing all **8** services
com.plugin.fcm.EdgeFirebaseMessagingService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **4** receivers
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

PROVIDERS

▼ Showing all **3** providers
org.apache.cordova.camera.FileProvider
com.google.firebase.provider.FirebaseInitProvider
androidx.startup.InitializationProvider

LIBRARIES

FILES

▶ Show all **2077** files

Version v4.0.7