ANDROID STATIC ANALYSIS REPORT

🤖 JazzCash (9.0.72)

File Name:	jazzcash.apk
Package Name:	com.techlogix.mobilinkcustomer
Scan Date:	Oct. 19, 2024, 10:48 a.m.
App Security Score:	**43/100 (MEDIUM RISK)**
Grade:	**B**
Trackers Detection:	11/432

📊 FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
11	26	3	4	2

📦 FILE INFORMATION

File Name: jazzcash.apk
Size: 62.97MB
MD5: 4929d2d02cebff1361627d8b2552ea86
SHA1: bdc61034c4742ba61639b55b58f2488902888fbc
SHA256: 773314532559d82a2419db04c6d027c5b51577df0fbb9aed569c2570e0222ea4

ℹ APP INFORMATION

App Name: JazzCash
Package Name: com.techlogix.mobilinkcustomer
Main Activity: com.ibm.jazzcashconsumer.view.splash.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 9.0.72

Android Version Code: 9072

▨ APP COMPONENTS

Activities: 196
Services: 26
Receivers: 22
Providers: 11
Exported Activities: 4
Exported Services: 4
Exported Receivers: 5
Exported Providers: 1

❋ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=PK, O=Mobilink, OU=MobicashCustomer, CN=Mobilink
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-05-16 14:37:28+00:00
Valid To: 2041-05-10 14:37:28+00:00
Issuer: C=PK, O=Mobilink, OU=MobicashCustomer, CN=Mobilink
Serial Number: 0x17e70e46
Hash Algorithm: sha256
md5: 23cf45f702800998913ec13fb67dfc68
sha1: 7554f7a1ae783c41351dc563a1d1fc4adead3e40
sha256: e6f0bdad0623e366fb79336e7b255ae7ebc6b8f4a96378b0e4f46ba60248760d
sha512: 0cb3da5f2c5a40964f1611f99c92867316d9a5e286ddf92144e865eb4bc5a51a9bc869ffcd343fe82dfaaa2349c43099dadce0a364fd98a180a783ee19396b4e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f5c9605be190a4e6c5451c973c472fe19288c8b459010bb44c0da57e9e6280fe
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
com.example.manyexampleapp.c2dm.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.techlogix.mobilinkcustomer.permission.PROCESS_PUSH_MSG	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.techlogix.mobilinkcustomer.permission.PUSH_PROVIDER	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

🔎 APKID ANALYSIS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check network operator name check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8

FILE	DETAILS	
classes2.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	network operator name check
	Compiler	r8
classes3.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check network operator name check
	Obfuscator	DexGuard
	Compiler	r8

FILE	DETAILS

classes4.dex		
	FINDINGS	**DETAILS**
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check ro.kernel.qemu check possible VM check
	Obfuscator	DexGuard
	Compiler	r8

classes5.dex		
	FINDINGS	**DETAILS**
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check SIM operator check ro.kernel.qemu check
	Obfuscator	DexGuard
	Compiler	r8

FILE	DETAILS		
classes6.dex	**FINDINGS**	**DETAILS**	
	Anti-VM Code	possible Build.SERIAL check Build.TAGS check	
	Obfuscator	DexGuard	
	Compiler	r8	

🗔 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ibm.jazzcashconsumer.view.splash.SplashActivity	Schemes: https://, jazzcash://, Hosts: jazzcashconsumer.page.link, www.jazzcash.com.pk, deeplink, Path Patterns: /deeplink,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.techlogix.mobilinkcustomer,

🔒 NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **1** | SECURE: **2**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*.jazzcash.com.pk	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
2	*.jazzcash.com.pk	info	Domain config is configured to trust bundled certs @raw/ssl_certificate.
3	*.jazzcash.com.pk	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: eIsBT7ALukWdTzVOIpNEJ7d29IKTHYKTMWTFQyhzYSs= Digest: SHA-256]
4	yayvo.com cdn.weatherapi.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

📇 CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.

🔍 MANIFEST ANALYSIS

HIGH: **3** | WARNING: **14** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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.
2	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.
3	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.
4	Activity (com.ibm.jazzcashconsumer.view.tapandpay.TapNPayActivity) is not Protected. [android:exported=true]	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.
5	Activity (com.ibm.jazzcashconsumer.view.raastqr.RaastQrGenerateActivity) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (com.ibm.jazzcashconsumer.view.sendmoney.raast.SendMoneyToRasstActivity) is not Protected. [android:exported=true]	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.
7	App Link assetlinks.json file not found [android:name=com.ibm.jazzcashconsumer.view.splash.SplashActivity] [android:host=https://www.jazzcash.com.pk]	high	App Link asset verification URL (https://www.jazzcash.com.pk/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
8	Broadcast Receiver (com.ibm.jazzcashconsumer.receivers.OtpBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.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 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.
9	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Service (com.ibm.jazzcashconsumer.services.WalletHceService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_SERVICE [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 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.
11	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 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.
12	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	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 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.
14	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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 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.
15	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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 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
16	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) is Protected by a permission. Permission: com.techlogix.mobilinkcustomer.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
17	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) is Protected by a permission. Permission: com.techlogix.mobilinkcustomer.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
18	Service (com.huawei.hms.support.api.push.service.HmsMsgService) is not Protected. [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.
19	Content Provider (com.huawei.hms.support.api.push.PushProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/huawei/agconnect/credential/obs/a.java com/huawei/agconnect/credential/obs/f.java com/huawei/agconnect/credential/obs/r.java com/huawei/hms/location/LocationAvailability.java com/huawei/hms/location/LocationResult.java com/huawei/hms/push/constant/RemoteMessageConst.java com/huawei/hms/support/hianalytics/HiAnalyticsConstant.java com/ibm/jazzcashconsumer/view/ktrade/dialog/forumdialog/KtradeAskQuestionDialog.java com/ibm/jazzcashconsumer/view/ktrade/dialog/profiledialog/KtradeLandingWelcomeDialog.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/defaultdata/securepreferences/SecurePreferences.java o/getNew_tag.java
				com/appsflyer/internal/AFa1cSDK.java com/appsflyer/internal/AFb1kSDK.java com/appsflyer/internal/AFc1iSDK.java com/appsflyer/internal/AFd1aSDK.java com/appsflyer/internal/AFd1bSDK.java com/appsflyer/internal/AFd1dSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFe1dSDK.java com/appsflyer/internal/AFe1pSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1tSDK.java com/appsflyer/internal/AFe1ySDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFe1zSDK.java com/appsflyer/internal/AFf1ySDK.java com/appsflyer/internal/AFg1jSDK.java
				com/bumptech/glide/Glide.java com/huawei/agconnect/credential/obs/h.java com/huawei/hms/aaid/HmsInstanceId.java com/huawei/hms/aaid/HmsInstanceIdEx.java com/huawei/hms/aaid/init/AutoInitHelper.java com/huawei/hms/aaid/utils/BaseUtils.java com/huawei/hms/aaid/utils/PushPreferences.java com/huawei/hms/activity/BridgeActivity.java com/huawei/hms/activity/ForegroundBusDelegate.java com/huawei/hms/activity/internal/ForegroundInnerHeader.java com/huawei/hms/adapter/AvailableAdapter.java com/huawei/hms/adapter/BaseAdapter.java com/huawei/hms/adapter/BinderAdapter.java com/huawei/hms/adapter/InnerBinderAdapter.java com/huawei/hms/adapter/OuterBinderAdapter.java com/huawei/hms/adapter/ui/BaseResolutionAdapter.java com/huawei/hms/adapter/ui/NotInstalledHmsAdapter.java com/huawei/hms/adapter/ui/UpdateAdapter.java com/huawei/hms/analytics/HiAnalyticsInstance.java com/huawei/hms/analytics/HiAnalyticsTools.java com/huawei/hms/analytics/a.java com/huawei/hms/analytics/aa.java com/huawei/hms/analytics/ab.java com/huawei/hms/analytics/abc.java com/huawei/hms/analytics/ac.java com/huawei/hms/analytics/ad.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/analytics/ae.java
				com/huawei/hms/analytics/ag.java
				com/huawei/hms/analytics/ah.java
				com/huawei/hms/analytics/ai.java
				com/huawei/hms/analytics/aj.java
				com/huawei/hms/analytics/ao.java
				com/huawei/hms/analytics/aq.java
				com/huawei/hms/analytics/au.java
				com/huawei/hms/analytics/ax.java
				com/huawei/hms/analytics/az.java
				com/huawei/hms/analytics/bb.java
				com/huawei/hms/analytics/bcd.java
				com/huawei/hms/analytics/be.java
				com/huawei/hms/analytics/bh.java
				com/huawei/hms/analytics/bl.java
				com/huawei/hms/analytics/bm.java
				com/huawei/hms/analytics/bn.java
				com/huawei/hms/analytics/bo.java
				com/huawei/hms/analytics/bp.java
				com/huawei/hms/analytics/bq.java
				com/huawei/hms/analytics/br.java
				com/huawei/hms/analytics/bs.java
				com/huawei/hms/analytics/bt.java
				com/huawei/hms/analytics/bu.java
				com/huawei/hms/analytics/bv.java
				com/huawei/hms/analytics/bw.java
				com/huawei/hms/analytics/bx.java
				com/huawei/hms/analytics/by.java
				com/huawei/hms/analytics/c.java
				com/huawei/hms/analytics/cb.java
				com/huawei/hms/analytics/cd.java
				com/huawei/hms/analytics/ce.java
				com/huawei/hms/analytics/cf.java
				com/huawei/hms/analytics/ci.java
				com/huawei/hms/analytics/cj.java
				com/huawei/hms/analytics/ck.java
				com/huawei/hms/analytics/cm.java
				com/huawei/hms/analytics/cn.java
				com/huawei/hms/analytics/co.java
				com/huawei/hms/analytics/connector/Connec

NO	ISSUE	SEVERITY	STANDARDS	FILES
				torManager.java com/huawei/hms/analytics/core/crypto/AesCipher.java com/huawei/hms/analytics/core/crypto/RsaCipher.java com/huawei/hms/analytics/core/storage/Event.java com/huawei/hms/analytics/core/transport/net/HttpTransportHandler.java com/huawei/hms/analytics/core/transport/net/a.java com/huawei/hms/analytics/cq.java com/huawei/hms/analytics/cr.java com/huawei/hms/analytics/cs.java com/huawei/hms/analytics/ct.java com/huawei/hms/analytics/cu.java com/huawei/hms/analytics/cx.java com/huawei/hms/analytics/cy.java com/huawei/hms/analytics/cz.java com/huawei/hms/analytics/database/DaoManager.java com/huawei/hms/analytics/database/LogEventDaoManager.java com/huawei/hms/analytics/db.java com/huawei/hms/analytics/de.java com/huawei/hms/analytics/dg.java com/huawei/hms/analytics/dh.java com/huawei/hms/analytics/dj.java com/huawei/hms/analytics/dk.java com/huawei/hms/analytics/e.java com/huawei/hms/analytics/f.java com/huawei/hms/analytics/framework/HAFrameworkInstance.java com/huawei/hms/analytics/framework/c/a.java com/huawei/hms/analytics/framework/c/a/c.java com/huawei/hms/analytics/framework/c/d.java com/huawei/hms/analytics/framework/c/e.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/analytics/framework/c/f.java
				com/huawei/hms/analytics/framework/c/g.java
				com/huawei/hms/analytics/framework/c/h.java
				com/huawei/hms/analytics/framework/c/i.java
				com/huawei/hms/analytics/framework/c/k.java
				com/huawei/hms/analytics/framework/e/b.java
				com/huawei/hms/analytics/framework/f/a.java
				com/huawei/hms/analytics/framework/g/a.java
				com/huawei/hms/analytics/g.java
				com/huawei/hms/analytics/ghi.java
				com/huawei/hms/analytics/hij.java
				com/huawei/hms/analytics/i.java
				com/huawei/hms/analytics/ijk.java
				com/huawei/hms/analytics/internal/filter/EventFilter.java
				com/huawei/hms/analytics/j.java
				com/huawei/hms/analytics/klm.java
				com/huawei/hms/analytics/l.java
				com/huawei/hms/analytics/o.java
				com/huawei/hms/analytics/provider/AnalyticsInitializeProvider.java
				com/huawei/hms/analytics/receiver/HiAnalyticsSvcEvtReceiver.java
				com/huawei/hms/analytics/s.java
				com/huawei/hms/analytics/t.java
				com/huawei/hms/analytics/type/ReportPolicy.java
				com/huawei/hms/analytics/u.java
				com/huawei/hms/analytics/w.java
				com/huawei/hms/analytics/x.java
				com/huawei/hms/android/SystemUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/api/BindingFailedResolution.java
				com/huawei/hms/api/FailedBinderCallBack.java
				com/huawei/hms/api/HuaweiApiClientImpl.java
				com/huawei/hms/api/HuaweiMobileServicesUtil.java
				com/huawei/hms/api/IPCCallback.java
				com/huawei/hms/api/IPCTransport.java
				com/huawei/hms/api/ResolutionDelegate.java
				com/huawei/hms/api/b.java
				com/huawei/hms/availableupdate/a.java
				com/huawei/hms/common/HuaweiApi.java
				com/huawei/hms/common/api/AvailabilityException.java
				com/huawei/hms/common/data/DataHolder.java
				com/huawei/hms/common/internal/BaseHmsClient.java
				com/huawei/hms/common/internal/ConnectionErrorMessages.java
				com/huawei/hms/common/internal/DialogRedirect.java
				com/huawei/hms/common/internal/HmsClient.java
				com/huawei/hms/common/internal/RequestHeader.java
				com/huawei/hms/common/internal/RequestManager.java
				com/huawei/hms/common/internal/ResponseHeader.java
				com/huawei/hms/common/internal/ResponseWrap.java
				com/huawei/hms/common/internal/TaskApiCall.java
				com/huawei/hms/common/util/AGCUtils.java
				com/huawei/hms/common/util/Base64Utils.java
				com/huawei/hms/common/util/Logger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/device/a.java com/huawei/hms/framework/common/Logger.java com/huawei/hms/hwid/as.java com/huawei/hms/locationSdk/a1.java com/huawei/hms/locationSdk/b0.java com/huawei/hms/locationSdk/b1.java com/huawei/hms/locationSdk/c0.java com/huawei/hms/locationSdk/c1.java com/huawei/hms/locationSdk/d.java com/huawei/hms/locationSdk/d1.java com/huawei/hms/locationSdk/e1.java com/huawei/hms/locationSdk/f.java com/huawei/hms/locationSdk/f0.java com/huawei/hms/locationSdk/f1.java com/huawei/hms/locationSdk/g.java com/huawei/hms/locationSdk/h0.java com/huawei/hms/locationSdk/h1.java com/huawei/hms/locationSdk/j.java com/huawei/hms/locationSdk/j0.java com/huawei/hms/locationSdk/j1.java com/huawei/hms/locationSdk/k0.java com/huawei/hms/locationSdk/k1.java com/huawei/hms/locationSdk/l0.java com/huawei/hms/locationSdk/m.java com/huawei/hms/locationSdk/m0.java com/huawei/hms/locationSdk/n0.java com/huawei/hms/locationSdk/o0.java com/huawei/hms/locationSdk/p.java com/huawei/hms/locationSdk/p0.java com/huawei/hms/locationSdk/q0.java com/huawei/hms/locationSdk/r0.java com/huawei/hms/locationSdk/s0.java com/huawei/hms/locationSdk/t0.java com/huawei/hms/locationSdk/u0.java com/huawei/hms/locationSdk/v0.java com/huawei/hms/locationSdk/w0.java com/huawei/hms/locationSdk/x0.java com/huawei/hms/locationSdk/y0.java com/huawei/hms/locationSdk/z0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/maps/utils/LogM.java com/huawei/hms/opendevice/OpenDeviceTas kApiCall.java
				com/huawei/hms/opendevice/c.java
				com/huawei/hms/opendevice/d.java
				com/huawei/hms/opendevice/e.java
				com/huawei/hms/opendevice/f.java
				com/huawei/hms/opendevice/g.java
				com/huawei/hms/opendevice/h.java
				com/huawei/hms/opendevice/i.java
				com/huawei/hms/opendevice/k.java
				com/huawei/hms/opendevice/l.java
				com/huawei/hms/opendevice/m.java
				com/huawei/hms/opendevice/n.java
				com/huawei/hms/opendevice/o.java
				com/huawei/hms/opendevice/p.java
				com/huawei/hms/opendevice/r.java
				com/huawei/hms/opendevice/s.java
				com/huawei/hms/push/HmsMessageService.j ava
				com/huawei/hms/push/HmsMessaging.java
				com/huawei/hms/push/HmsProfile.java
				com/huawei/hms/push/RemoteMessage.java
				com/huawei/hms/push/c.java
				com/huawei/hms/push/d.java
				com/huawei/hms/push/e.java
				com/huawei/hms/push/g.java
				com/huawei/hms/push/h.java
				com/huawei/hms/push/i.java
				com/huawei/hms/push/j.java
				com/huawei/hms/push/k.java
				com/huawei/hms/push/l.java
				com/huawei/hms/push/o.java
				com/huawei/hms/push/p.java
				com/huawei/hms/push/q.java
				com/huawei/hms/push/r.java
				com/huawei/hms/push/s.java
				com/huawei/hms/push/task/BaseVoidTask.jav a
				com/huawei/hms/push/task/SendUpStreamTa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sk.java
				com/huawei/hms/push/ups/UPSService.java
				com/huawei/hms/push/utils/DateUtil.java
2	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	com/huawei/hms/push/utils/JsonUtil.java com/huawei/hms/push/utils/PluginUtil.java com/huawei/hms/stats/a.java com/huawei/hms/stats/c.java com/huawei/hms/support/api/ErrorResultImpl.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/api/client/ResolvingResultCallbacks.java com/huawei/hms/support/api/client/ResultCallbacks.java com/huawei/hms/support/api/core/ConnectService.java com/huawei/hms/support/api/location/common/HMSLocationLog.java com/huawei/hms/support/api/location/common/LocationClientStateManager.java com/huawei/hms/support/api/location/common/PermissionUtil.java com/huawei/hms/support/api/location/common/exception/ServiceErrorCodeAdaptor.java com/huawei/hms/support/api/push/PushMsgReceiver.java com/huawei/hms/support/api/push/PushProvider.java com/huawei/hms/support/api/push/PushReceiver.java com/huawei/hms/support/api/push/service/HmsMsgService.java com/huawei/hms/support/common/ActivityMgr.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/HiAnalyticsUtils.java com/huawei/hms/support/log/HMSDebugger.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava
				com/huawei/hms/ui/AbstractDialog.java
				com/huawei/hms/update/note/AppSpoofResolution.java
				com/huawei/hms/update/note/DoNothingResolution.java
				com/huawei/hms/update/note/NotInstalledHmsResolution.java
				com/huawei/hms/update/ui/NotInstalledHmsDialogHelper.java
				com/huawei/hms/utils/FileUtil.java
				com/huawei/hms/utils/HMSBIInitializer.java
				com/huawei/hms/utils/HMSPackageManager.java
				com/huawei/hms/utils/IOUtils.java
				com/huawei/hms/utils/JsonUtil.java
				com/huawei/hms/utils/PackageManagerHelper.java
				com/huawei/hms/utils/ReadApkFileUtil.java
				com/huawei/hms/utils/SHA256.java
				com/huawei/hms/utils/UIUtil.java
				com/huawei/hms/utils/Util.java
				com/ibm/jazzcashconsumer/JazzCashApplication.java
				com/ibm/jazzcashconsumer/view/alfalahintegration/fragments/ReviewBankUserDetailsFragment.java
				com/ibm/jazzcashconsumer/view/m2c/dashboard/khata/AllUserKhataFragment.java
				com/ibm/jazzcashconsumer/view/payoneer/previoustransaction/PreviousTransactionsFragment.java
				o/AlarmManagerSchedulerBroadcastReceiver.java
				o/AppBarLayoutBehavior.java
				o/AutocompleteActivity.java
				o/AutocompleteImplFragmentzzb.java
				o/AutocompleteSupportFragment.java
				o/BaseRequestDelegate.java
				o/BaseRequestFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/BiometricGuideFragment.java
				o/BuildConfig.java
				o/ByteArrayPool1.java
				o/CancelPendingTransactionRequestParams.java
				o/CropInsuranceCropTypeParams.java
				o/CropInsuranceDraftPolicyParams.java
				o/CropInsuranceTypeRequestFactory.java
				o/CropInsuranceWeatherRequestFactory.java
				o/CropPolicyIssueRequestFactory.java
				o/DarazInitRequestFactory.java
				o/DarazInitRequestParams.java
				o/EditPayerRequest.java
				o/EditPayerRequestCreator.java
				o/EligibilityAmountCreator.java
				o/FileClaimRequestFactory.java
				o/FirebaseInAppMessagingDisplayRegistrar.java
				o/FromCreator.java
				o/GetAllPayerRequestFactory.java
				o/GpsAlmItem.java
				o/GpsUtc.java
				o/GuestLoginRequestParams.java
				o/HuaweiMap23.java
				o/IRouterResponse.java
				o/InstallReferrerClient.java
				o/InstallReferrerClientImplClientState.java
				o/InsuranceMyClaimsRequestCreator.java
				o/InsuranceMyClaimsRequestFactory.java
				o/KpmsConstant.java
				o/KtradeWatchlistDeleteRequestFactory.java
				o/KtradeWatchlistRequestFactory.java
				o/ListChangeRegistryListChanges.java
				o/LoanInquiryItem.java
				o/LoanRepaymentItemCreator.java
				o/LoanRequestRequestFactory.java
				o/LocationStatusCode.java
				o/MainThread.java
				o/MaterialDatePicker.java
				o/MaterialTextView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/MiniCircleImageView.java o/ManualLayoutPortrait.java o/MovementEvent.java
				o/MtagRuleEngineRequestParam.java o/NanoLoanEligibilityResponseCreator.java o/Network.java o/NetworkResponse.java o/NewPaymentRequest.java o/NewPaymentRequestCreator.java o/NoConnectionError.java o/OpenDeviceHmsClientBuilder.java o/OrderInProgressData.java o/ParcelableSparseBooleanArray.java o/PromotionBannerRequestParams.java o/PropertyGetterDescriptorImpl.java o/PropertySetterDescriptorImpl.java o/QuietHACapabilityImpl.java o/RadialViewGroup.java o/ReceiverParameterDescriptorImpl.java o/ReferAndWinReminderFragment.java o/ReflectKotlinClassFinder.java o/RemoteMessage.java o/RemoteMessageConstNotification.java o/RequestMoneyFromFriendPramsCreator.java o/RequestMoneyReminderRequest.java o/RequestQueue.java o/StreetViewPanoramaCamera.java o/StreetViewPanoramaOrientation.java o/ViewDataBinding1.java o/VolleyLogMarkerLogMarker.java o/WelcomeBannerRequestParams.java o/aBdsNav.java o/access802.java o/aesKsDecrypt.java o/afErrorLogForExcManagerOnly.java o/bd.java o/beforeTextChanged.java o/bf.java o/boundsNullability.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/checkNonZero.java
				o/cloneable.java
				o/compareTo.java
				o/component27.java
				o/cp.java
				o/createErrorProperty.java
				o/createErrorTypeConstructor.java
				o/detectComponents.java
				o/dfs.java
				o/dismissWithAnimation.java
				o/getAccountHolderName.java
				o/getApiRequestMap.java
				o/getAppCertFP.java
				o/getC2gAmountSent.java
				o/getCacheKey.java
				o/getClientName.java
				o/getCvrMaskAnd.java
				o/getDesc.java
				o/getDq.java
				o/getExitTransition.java
				o/getFarmSize.java
				o/getFavouriteList.java
				o/getFlagsFilter.java
				o/getFullInterSignalBiasUncertaintyNanos.java
				o/getGalTim.java
				o/getGrant_type.java
				o/getHeads.java
				o/getI0.java
				o/getIdId.java
				o/getLocality.java
				o/getManufacturer.java
				o/getMaximumAmount.java
				o/getMessageId.java
				o/getName.java
				o/getOmega0.java
				o/getOmegaDot.java
				o/getPolicy.java
				o/getRequestMoneyFromFriends.java
				o/getStatusFromIntent.java
				o/getTransformation3DESPreProd.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/getU.java
				o/hasAttemptRemaining.java
				o/hasHadResponseDelivered.java
				o/initVdrDataManager.java
				o/internalGetViewDataBinding0.java
				o/internalGetViewDataBinding10.java
				o/internalPopulateLayoutIdLookup1.java
				o/isErrorTypeEqualsToAnything.java
				o/isLowEmuiVersion.java
				o/isNeedCheckAGC.java
				o/isPackageFreshInstall.java
				o/isSuccess.java
				o/notifyChange.java
				o/onCallBackSuccess.java
				o/onInstallReferrerSetupFinished.java
				o/onKey.java
				o/realEnquene.java
				o/registerToken.java
				o/resetForTesting.java
				o/rewriteUrl.java
				o/sdmProcess.java
				o/sdmUpdateEphemeris.java
				o/setAcc.java
				o/setAccessible.java
				o/setApiRequest.java
				o/setBackgroundTintList.java
				o/setBoxStrokeWidth.java
				o/setCheckedIconVisible.java
				o/setCityCode.java
				o/setCollectIMEI.java
				o/setCradleVerticalOffset.java
				o/setCropType.java
				o/setDebugLog.java
				o/setDepartureCityId.java
				o/setExpandedTitleColor.java
				o/setExpandedTitleTextAppearance.java
				o/setFallbackResource.java
				o/setFarmAddress.java
				o/setFontAssetDelegate.java
				o/setHyphenationFrequency.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/setItemIconSizeRes.java o/setLoanOutstanding.java o/setMaxInlineActionWidth.java o/setMaxWidthResource.java o/setMerchantAmount.java o/setMinSeparation.java o/setNeighborCells.java o/setPlayer.java o/setProceed.java o/setResponseBytes.java o/setScale.java o/setScrimsShown.java o/setScrubberColor.java o/setShowBuffering.java o/setSizeOptions.java o/setStartIconCheckable.java o/setStartIconOnClickListener.java o/setStartIconVisible.java o/setStatusBarScrimResource.java o/setTitleCentered.java o/setTitleEnabled.java o/setTitleMarginStart.java o/setUserData.java o/setValues.java o/updateRootKey.java o/withAcc.java o/withAlg.java o/withBiasUncertaintyNanos.java o/zzgi.java o/zzjhzzd.java o/zzjjzzb.java o/zzjozzn.java o/zzkfzzhzza.java o/zzkfzzkzza.java o/zzki.java o/zzkl.java o/zzkm.java o/zzko.java o/zzkozzazza.java o/zzkt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/zzkvzzk.java o/zzzszzd.java o/zzkx.java o/zzky.java o/zzlz.java o/zzmb.java o/zzmd.java o/zzmi.java o/zzmqzzag.java o/zzmqzzahzzb.java o/zzmqzzai.java o/zzmqzzal.java o/zzmqzzb.java o/zzmqzzczza.java o/zzmqzzizzd.java o/zzmqzzj.java o/zzmqzzk.java o/zzmqzzkzza.java o/zzmqzzl.java o/zzmqzzn.java o/zzmqzzp.java o/zzmqzzqzzb.java o/zznr.java o/zzob.java o/zzoe.java o/zzoj.java o/zzot.java
				o/zzoz.java o/zzpd.java o/zzqd.java o/zzqgzzb.java o/zzqkzzb.java o/zzqx.java o/zzru.java o/zzsb.java o/zzth.java o/zztx.java o/zztz.java o/zzux.java o/zzvczza.java c/o/w.java com/appsflyer/internal/AFa1ySDK.java com/huawei/hms/common/internal/TransactionIdCreater.java com/huawei/hms/support/hwid/service/HuaweiIdAuthAPIServiceImpl.java com/ibm/jazzcashconsumer/view/ktrade/KTradeBaseFragment.java o/DescriptorRendererCompanionCOMPACT1.java o/DescriptorRendererCompanionCOMPACT_WITHOUT_SUPERTYPES1.java o/DescriptorRendererCompanionCOMPACT_W

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ITH_MODIFIERS1.java o/FullSavedBillRequestFactory.java o/EventTicketPassCreator.java
3	[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	o/FullJazzInitResponseData.java o/LazyJavaResolverContext.java o/MultipleInstallBroadcastReceiver.java o/NavigationMenuItemView.java o/NullabilityChecker.java o/OmnoMpinRequestFactory.java o/ProtoBufAnnotationArgument1.java o/ProtoBufTypeAlias.java o/ProtoBufVersionRequirementOrBuilder.java o/Slide.java o/StrictEqualityTypeChecker.java o/access17202.java o/access18500.java o/access21400.java o/access8500.java o/accesssearchMethodsInSupertypesWithoutBuiltinMagic.java o/createInputStream.java o/dispatchTouchEvent.java o/getAddParameters.java o/getClientInfo.java o/getLastCustomNonConfigurationInstance.java o/getReified.java o/hasTopLevelClass.java o/setCreatedBy.java o/setFloorAcc.java o/set__v.java o/withA3.java o/withAlg.java o/zzcc.java o/zzjazzc.java
				com/huawei/agconnect/credential/BuildConfig.java com/huawei/agconnect/credential/obs/ai.java com/huawei/agconnect/credential/obs/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/huawei/agconnect/datastore/BuildConfig.java com/huawei/hms/analytics/bo.java com/huawei/hms/analytics/bz.java com/huawei/hms/analytics/co.java com/huawei/hms/analytics/dd.java com/huawei/hms/analytics/framework/c/i.java com/huawei/hms/analytics/hij.java com/huawei/hms/api/HuaweiApiAvailability.java com/huawei/hms/api/HuaweiApiClientImpl.java com/huawei/hms/base/device/BuildConfig.java com/huawei/hms/common/PackageConstants.java com/huawei/hms/feature/dynamic/a.java com/huawei/hms/framework/common/BuildConfig.java com/huawei/hms/framework/common/PackageManagerCompat.java com/huawei/hms/framework/common/hianalytics/HianalyticsHelper.java com/huawei/hms/framework/network/frameworkcompat/BuildConfig.java com/huawei/hms/framework/network/grs/BuildConfig.java com/huawei/hms/framework/network/grs/g/k/a.java com/huawei/hms/framework/network/grs/h/a.java com/huawei/hms/hatool/g1.java com/huawei/hms/hatool/v.java com/huawei/hms/hatool/z.java com/huawei/hms/hwid/e.java com/huawei/hms/hwid/w.java com/huawei/hms/location/BuildConfig.java com/huawei/hms/location/base/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/maps/api/BuildConfig.java com/huawei/hms/maps/common/util/mab.java com/huawei/hms/maps/internal/HmsUtil.java com/huawei/hms/opendevice/o.java com/huawei/hms/site/api/BuildConfig.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/a.java com/huawei/hms/support/hwid/service/HuaweiIdAuthAPIServiceImpl.java com/huawei/location/router/BuildConfig.java com/huawei/wisesecurity/ucs/credential/CredentialClient.java o/UnresolvedType.java o/WrappedType.java o/debugInfo.java o/getSendInvitationFrequencyMax.java o/inheritEnhancement.java o/isSingleClassifierTypeWithEnhancement.java o/setQrDiscountUrl.java o/unwrapEnhancement.java o/withFlexibility.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	[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	com/huawei/agconnect/credential/obs/ab.java com/huawei/agconnect/credential/obs/f.java com/huawei/hms/ads/identifier/d.java com/huawei/hms/analytics/af.java com/huawei/hms/hatool/e.java com/huawei/hms/site/C0210r.java com/veridiumid/sdk/model/help/EncryptionUtils.java o/AFa1aSDK.java o/LazyJavaPackageFragmentpartToFacade2WhenMappings.java o/LazyJavaResolverContext.java o/accesssearchMethodsInSupertypesWithoutBuiltinMagic.java o/createPropertyDescriptorWithDefaultGetterdefault.java o/getDaysOverDue.java o/getJPayGetTrustIdentityRequestParams.java o/getNaturalDeath.java o/getPerTransactionLimitConfigurationsRaast.java o/getVisitedTypeParameters.java o/isSseSupported.java o/setDenominationAmount.java o/setFile5InBase64.java o/setPostition.java o/setYearlyReceivingLimit.java
				o/AlphaNanoLoanKYCFormRequestFactory.java o/DarazConfirmRequestParamsCreator.java o/DarazInitRequestParams.java o/EventConfirmRequestFactory.java o/JavaNullabilityAnnotationsStatusCompanion.java o/JavaTypeEnhancementState.java o/LazyJavaClassMemberScopecomputeNonDe

NO	ISSUE	SEVERITY	STANDARDS	FILES
				claredFunctions3.java o/...siInstanceInvalidationService.java o/RegisterOmnoRequestFactory.java
6	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	o/RegisterUssdRequestParamsCreator.java o/SlidingPaneLayout.java o/SmartSet.java o/StaggeredGridLayoutManagerLayoutParams .java o/VerifyOtpRequestFactory.java o/accessgetJClassp.java o/accesssearchMethodsByNameWithoutBuilti nMagic.java o/addFunctionFromSupertypes.java o/addOverriddenSpecialMethods.java o/addPropertyOverrideByMethod.java o/checkLocationSettings.java o/computeAnnotationProperties.java o/getDEFAULT.java o/getDefaultQualifiers.java o/getFavouriteList.java o/getReportLevelAfter.java o/getReportLevelForAnnotationdefault.java o/isSafeToMultiply.java o/setActivityTransitionResult.java o/setCnicBackUrl.java o/setHMSLocationPresent.java o/setKeepContentOnPlayerReset.java o/setNote.java o/setRepaymentAmount.java o/setShowBuffering.java o/upTo.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	com/huawei/hms/analytics/db.java com/ibm/jazzcashconsumer/view/depositmoney/debitcard/scandebitcard/ScanDebitCardFragment.java com/ibm/jazzcashconsumer/view/main/home/HomeFragment.java com/ibm/jazzcashconsumer/view/registration/account_registration/scancnic/ScanCnicFragment.java com/ibm/jazzcashconsumer/view/registration/scan/personalphoto/PersonalPhotoFragment.java com/ibm/jazzcashconsumer/view/registration/scan/scancnic/ScanCnicFragment.java com/ibm/jazzcashconsumer/view/visa/cardordering/success/CardOrderingSuccessFragment.java com/unikrew/faceoff/fingerprint/FingerprintScannerActivity.java com/veridiumid/sdk/fourf/camera/FourFCamera2.java o/BankingAppMobileDcCloudMessagingConfigurationgetProvider1.java o/InflatedUIStates.java o/JsonReader.java o/MultipleInstallBroadcastReceiver.java o/OtpBroadcastReceiver.java o/setBorderColor.java o/setHeaderAaId.java o/substituteSimpleType.java o/throttle.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/ibm/jazzcashconsumer/testingwebview/WebviewShow.java com/ibm/jazzcashconsumer/view/bookme/BookMeActivity.java com/pierfrancescosoffritti/androidyoutubeplayer/core/player/views/LegacyYouTubePlayerView.java o/getUserProfile.java
9	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	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	o/setTemplate.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java o/GetAllPayerRequestFactory.java o/LoyaltyPointRedeemOmnoPrePostFactory.java o/getClientName.java o/internalGetViewDataBinding10.java o/setMatchedKeywords.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/ibm/jazzcashconsumer/view/raastidmanagement/CreateRaastIdFragment.java com/ibm/jazzcashconsumer/view/util/AddAccountKeyboardFragment.java com/ibm/jazzcashconsumer/view/util/AddAmountKeyboardFragment.java com/ibm/jazzcashconsumer/view/util/AddPhoneKeyboardFragment.java com/ibm/jazzcashconsumer/view/util/CnicKeyboardFragment.java o/FcmTokenProvidergetFcmRegistrationTokenBlocking1.java
12	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	com/theartofdev/edmodo/cropper/CropImageActivity.java o/FragmentManager6.java o/InflatedUIStates.java o/PredefinedEnhancementInfoKtPREDEFINED_FUNCTION_ENHANCEMENT_INFO_BY_SIGNATURE11141.java o/beforeTextChanged.java o/getDueDateTill.java o/getParentFragment.java o/setNavigationIcon.java o/substituteSimpleType.java
13	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ibm/jazzcashconsumer/view/account/account_upgrade/UpgradeAccountActivity.java com/ibm/jazzcashconsumer/view/mtag/fragment/EnterMtagIdFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	[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/ibm/jazzcashconsumer/view/alfananoloan/activities/AlphaNanoLoanTermsActivity.java com/ibm/jazzcashconsumer/view/depositmoney/debitcard/DepositMoneyAddCardAuthorizeFragment.java com/ibm/jazzcashconsumer/view/entertainment/movietickets/fragment/BuyMovieTicketFragment.java com/ibm/jazzcashconsumer/view/insurance/ui/InsuranceBenefitsBottomSheetFragment.java com/ibm/jazzcashconsumer/view/insurance/ui/InsuranceSubscriptionFragment.java com/ibm/jazzcashconsumer/view/main/QrDiscountActivity.java com/ibm/jazzcashconsumer/view/payoneer/PayoneerWebview.java com/ibm/jazzcashconsumer/view/payoneer/fundstransfer/confirm/PayoneerWebviewForMFA.java o/ReferAndWinReminderFragment.java
15	[MD5 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	o/EditSavedBillRequestFactory.java o/PickerFragment.java o/TypeAdapters13.java o/cn.java o/createSuspendView.java o/getHostName.java o/rewriteUrl.java o/setColorSchemeColors.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/huawei/agconnect/credential/obs/ah.java com/ibm/jazzcashconsumer/model/retrofit/Service.java com/veridiumid/sdk/internal/licensing/ws/LicensingServiceApi.java o/ErrorType.java o/createErrorClass.java o/createErrorFunction.java o/createErrorType.java o/getQrDiscountUrl.java o/writeTo.java
17	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/huawei/agconnect/credential/obs/z.java o/AppCompatDialogFragment.java o/LazyJavaScopepropertyNamesLazy2.java o/ScrimInsetsFrameLayout.java o/getMaxTravelFavoriteLimit.java o/setPostition.java o/zzdr.java
18	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/huawei/agconnect/datastore/core/SharedPrefUtil.java com/unikrew/faceoff/fingerprint/SecureStorage/c.java o/accesssearchMethodsByNameWithoutBuiltinMagic.java
19	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	o/accesssearchMethodsInSupertypesWithoutBuiltinMagic.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
20	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/veridiumid/sdk/model/help/AndroidHelper.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/24	android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE
Other Common Permissions	6/45	android.permission.BLUETOOTH, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE, android.permission.CHANGE_WIFI_STATE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗ OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sregister.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.
app-measurement.com	ok	**IP:** 172.217.19.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
after.start	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **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
firebase-settings.crashlytics.com	ok	**IP:** 142.250.76.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.opensource.org	ok	**IP:** 104.21.84.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.250.192.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
api-gw.jazzcash.com.pk	ok	**IP:** 119.160.115.112 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** [Google Map](#)
www.google.com	ok	**IP:** 172.217.19.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
sapp.s	ok	No Geolocation information available.
unikrew-faceoff-licensing.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
login.payoneer.com	ok	**IP:** 35.190.33.81 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
services.upaid.pl	ok	**IP:** 46.229.151.108 **Country:** Poland **Region:** Mazowieckie **City:** Warsaw **Latitude:** 52.229771 **Longitude:** 21.011780 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
portallapp.page.link	ok	**IP:** 172.217.174.225 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
admob-gmats.uc.r.appspot.com	ok	**IP:** 142.250.71.116 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
faceoffmobilebackend.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** [Google Map](#)
anysoftkeyboard.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
image.eum-appdynamics.com	ok	**IP:** 44.241.145.66 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
plus.google.com	ok	**IP:** 142.250.183.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
staging.go-games.gg	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
svalidate.s	ok	No Geolocation information available.
faceoffauthentication.azurewebsites.net	ok	**IP:** 13.77.82.141 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
graph-video.s	ok	No Geolocation information available.
payoneer-integration-take-3.us-south.cf.appdomain.cloud	ok	No Geolocation information available.
console.firebase.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
ns.adobe.com	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
googlemobileadssdk.page.link	ok	**IP:** 172.217.174.225 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** [Google Map](#)
s.evendanan.net	ok	**IP:** 142.250.183.147 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
sattr.s	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.who.int	ok	**IP:** 192.133.11.1 **Country:** United States of America **Region:** Massachusetts **City:** Lexington **Latitude:** 42.445580 **Longitude:** -71.236221 **View:** Google Map
csi.gstatic.com	ok	**IP:** 216.239.32.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 172.217.17.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fonts.googleapis.com	ok	**IP:** 142.250.181.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ssdk-services.s	ok	No Geolocation information available.
support.google.com	ok	**IP:** 142.250.183.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.android.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
uniquelink.com	ok	**IP:** 149.28.121.93 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
send-beacons.com	ok	No Geolocation information available.
adservice.google.com	ok	**IP:** 172.217.19.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.jazzcash.com.pk	ok	**IP:** 67.225.171.21 **Country:** United States of America **Region:** Michigan **City:** Lansing **Latitude:** 42.733280 **Longitude:** -84.637764 **View:** Google Map
googleads.g.doubleclick.net	ok	**IP:** 142.250.70.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
licensing.prod.veridium-dev.com	ok	**IP:** 3.64.32.202 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
google.com	ok	**IP:** 142.250.181.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseremoteconfig.googleapis.com	ok	**IP:** 142.250.181.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
greenrobot.org	ok	**IP:** 85.13.163.69 **Country:** Germany **Region:** Thuringen **City:** Friedersdorf **Latitude:** 50.604919 **Longitude:** 11.035770 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
appgallery.cloud.huawei.com	ok	**IP:** 159.138.86.75 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
image.tmdb.org	ok	**IP:** 84.17.38.228 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
schemas.microsoft.com	ok	**IP:** 13.107.246.63 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
imasdk.googleapis.com	ok	**IP:** 142.250.67.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 142.250.192.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.google.com	ok	**IP:** 142.250.182.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sviap.s	ok	No Geolocation information available.
mobile.eum-appdynamics.com	ok	**IP:** 18.246.204.85 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.183.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

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
f-droid.org	ok	**IP:** 65.21.79.229 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
developer.android.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
sgcdsdk.s	ok	No Geolocation information available.
unikrew-faceoff-telemetry.azurewebsites.net	ok	**IP:** 65.52.250.96 **Country:** United Arab Emirates **Region:** Dubayy **City:** Dubai **Latitude:** 25.258169 **Longitude:** 55.304722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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](#)
facebook.com	ok	**IP:** 157.240.227.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** [Google Map](#)
www.huawei.com	ok	**IP:** 104.108.234.109 **Country:** India **Region:** Delhi **City:** New Delhi **Latitude:** 28.635759 **Longitude:** 77.224449 **View:** [Google Map](#)
apps.apple.com	ok	**IP:** 104.65.228.26 **Country:** India **Region:** Delhi **City:** New Delhi **Latitude:** 28.635759 **Longitude:** 77.224449 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
firebase.google.com	ok	**IP:** 142.250.183.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
api-gw-test.jazzcash.com.pk	ok	**IP:** 119.73.65.216 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** [Google Map](#)
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** [Google Map](#)
meezan-faceoff-backend.covalent.pk	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
scdn-ssettings.s	ok	No Geolocation information available.
exoplayer.dev	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
commons.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
pagead2.googlesyndication.com	ok	**IP:** 172.217.19.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.facebook.com	ok	**IP:** 157.240.227.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
meezan-faceoff-ids.covalent.pk	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
info@salaamtakaful.com	com/ibm/jazzcashconsumer/view/insurance/ui/claims/GeneralPolicyClaimFragment.java
u0013android@android.com u0013android@android.com0	o/zzny.java
waseem@gmail.com atif@gmail.com usama@gmail.com	o/getOriginalSetter.java
spapadim@cs.cmu ali@jazzcash.com email@website.com name@domain.com supersheets@gmail.com sheets@gmail.com yourname@website.com	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Appdynamics	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/194
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"abbreviation_dict_editor_key" : "abbreviation_dict_editor_key"

POSSIBLE SECRETS

"authorized_key" : "authorized_key"

"google_api_key" : "AIzaSyCEbWfYmLd4N8ad8pD34kBqZiyLKFEWTtQ"

"google_crash_reporting_api_key" : "AIzaSyCEbWfYmLd4N8ad8pD34kBqZiyLKFEWTtQ"

"google_maps_key" : "AIzaSyCEbWfYmLd4N8ad8pD34kBqZiyLKFEWTtQ"

"image_picker_provider_authority_suffix" : ".imagepicker.provider"

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"maxipanel_token" : "53b83078ab7055917f33cf49a11378b6"

"next_word_dict_settings_key" : "next_word_dict_settings_key"

"places_key" : "AIzaSyDpgm3uEvKDbexB6klZFrUZsjXVnjMqaCQ"

"settings_default_ext_kbd_bottom_row_key" : "09f8f280-dee2-11e0-9572-0800200c9a55"

"settings_default_ext_keyboard_key" : "6f1ecea0-dee2-11e0-9572-0800200c9a66"

"settings_default_key_press_preview_popup_position" : "above_key"

"settings_default_keyboard_theme_key" : "18c558ef-bc8c-433a-a36e-92c3ca3be4dd"

"settings_default_top_row_key" : "82910c70-ded1-11e0-9572-0800200c9a66"

"settings_key_allow_layouts_to_provide_generic_rows" : "settings_key_allow_layouts_to_provide_generic_rows"

POSSIBLE SECRETS
"settings_key_allow_suggestions_restart" : "settings_key_allow_suggestions_restart"
"settings_key_always_use_fallback_user_dictionary" : "settings_key_always_use_fallback_user_dictionary"
"settings_key_apply_remote_app_colors" : "settings_key_apply_remote_app_colors"
"settings_key_auto_capitalization" : "auto_caps"
"settings_key_auto_space" : "insert_space_after_word_suggestion_selection"
"settings_key_bool_should_swap_punctuation_and_space" : "settings_key_bool_should_swap_punctuation_and_space"
"settings_key_colorize_nav_bar" : "settings_key_colorize_nav_bar"
"settings_key_custom_sound_volume" : "custom_sound_volume"
"settings_key_cycle_all_symbols" : "settings_key_cycle_all_symbols"
"settings_key_default_emoji_skin_tone" : "settings_key_default_emoji_skin_tone"
"settings_key_default_split_state_landscape" : "settings_key_default_split_state_landscape"
"settings_key_default_split_state_portrait" : "settings_key_default_split_state_portrait"
"settings_key_do_not_flip_quick_key_codes_functionality" : "settings_key_do_not_flip_quick_key_codes_functionality"
"settings_key_double_space_to_period" : "double_space_to_period"
"settings_key_enable_alt_space_language_shortcut" : "settings_key_enable_alt_space_language_shortcut"

POSSIBLE SECRETS
"settings_key_enable_shift_space_language_shortcut" : "settings_key_enable_shift_space_language_shortcut"
"settings_key_extension_keyboard_enabled" : "settings_key_extension_keyboard_enabled"
"settings_key_force_locale" : "settings_key_force_locale"
"settings_key_gesture_typing" : "settings_key_gesture_typing"
"settings_key_is_sticky_extesion_keyboard" : "settings_key_is_sticky_extesion_keyboard"
"settings_key_key_press_preview_popup_position" : "settings_key_key_press_preview_popup_position"
"settings_key_key_press_shows_preview_popup" : "key_press_preview_popup"
"settings_key_keyboard_icon_in_status_bar" : "settings_key_keyboard_icon_in_status_bar"
"settings_key_landscape_fullscreen" : "settings_key_landscape_fullscreen"
"settings_key_landscape_keyboard_height_factor" : "zoom_factor_keys_in_landscape"
"settings_key_lang_key_shows_popup" : "lang_key_shows_popup"
"settings_key_layout_for_internet_fields" : "settings_key_layout_for_internet_fields"
"settings_key_long_press_timeout" : "settings_key_long_press_timeout"
"settings_key_min_length_for_word_correction__" : "settings_key_min_length_for_word_correction__"
"settings_key_multitap_timeout" : "settings_key_multitap_timeout"

POSSIBLE SECRETS

"settings_key_night_mode" : "settings_key_night_mode"

"settings_key_night_mode_app_theme_control" : "settings_key_night_mode_app_theme_control"

"settings_key_night_mode_sound_control" : "settings_key_night_mode_sound_control"

"settings_key_night_mode_theme_control" : "settings_key_night_mode_theme_control"

"settings_key_night_mode_vibration_control" : "settings_key_night_mode_vibration_control"

"settings_key_os_clipboard_sync" : "settings_key_os_clipboard_sync"

"settings_key_persistent_layout_per_package_id" : "settings_key_persistent_layout_per_package_id"

"settings_key_persistent_layout_per_package_id_mapping" : "settings_key_persistent_layout_per_package_id_mapping"

"settings_key_pinch_gesture_action" : "settings_key_pinch_gesture_action"

"settings_key_portrait_fullscreen" : "settings_key_portrait_fullscreen"

"settings_key_portrait_keyboard_height_factor" : "zoom_factor_keys_in_portrait"

"settings_key_power_save_mode" : "settings_key_power_save_mode"

"settings_key_power_save_mode_animation_control" : "settings_key_power_save_mode_animation_control"

"settings_key_power_save_mode_gesture_control" : "settings_key_power_save_mode_gesture_control"

"settings_key_power_save_mode_sound_control" : "settings_key_power_save_mode_sound_control"

POSSIBLE SECRETS

"settings_key_power_save_mode_suggestions_control" : "settings_key_power_save_mode_suggestions_control"

"settings_key_power_save_mode_theme_control" : "settings_key_power_save_mode_theme_control"

"settings_key_power_save_mode_vibration_control" : "settings_key_power_save_mode_vibration_control"

"settings_key_quick_fix" : "quick_fix"

"settings_key_quick_fix_second_disabled" : "settings_key_quick_fix_second_disabled"

"settings_key_separate_gesture_action" : "settings_key_separate_gesture_action"

"settings_key_show_chewbacca" : "settings_key_show_chewbacca"

"settings_key_show_settings_app" : "settings_key_show_settings_app"

"settings_key_show_suggestions" : "candidates_on"

"settings_key_smiley_icon_on_smileys_key" : "settings_key_smiley_icon_on_smileys_key"

"settings_key_sound_on" : "sound_on"

"settings_key_support_keyboard_type_state_row_type_2" : "settings_key_support_keyboard_type_state_row_type_2"

"settings_key_support_keyboard_type_state_row_type_3" : "settings_key_support_keyboard_type_state_row_type_3"

"settings_key_support_keyboard_type_state_row_type_4" : "settings_key_support_keyboard_type_state_row_type_4"

"settings_key_support_keyboard_type_state_row_type_5" : "settings_key_support_keyboard_type_state_row_type_5"

POSSIBLE SECRETS
"settings_key_swipe_down_action" : "settings_key_swipe_down_action"
"settings_key_swipe_left_action" : "settings_key_swipe_left_action"
"settings_key_swipe_left_space_bar_action" : "settings_key_swipe_left_space_bar_action"
"settings_key_swipe_left_two_fingers_action" : "settings_key_swipe_left_two_fingers_action"
"settings_key_swipe_right_action" : "settings_key_swipe_right_action"
"settings_key_swipe_right_space_bar_action" : "settings_key_swipe_right_space_bar_action"
"settings_key_swipe_right_two_fingers_action" : "settings_key_swipe_right_two_fingers_action"
"settings_key_swipe_up_action" : "settings_key_swipe_up_action"
"settings_key_swipe_up_from_spacebar_action" : "settings_key_swipe_up_from_spacebar_action"
"settings_key_switch_keyboard_on_space" : "settings_key_switch_keyboard_on_space"
"settings_key_theme_case_type_override" : "settings_key_theme_case_type_override"
"settings_key_tweak_animations_level" : "settings_key_tweak_animations_level"
"settings_key_use_16_keys_symbols_keyboards" : "settings_key_use_16_keys_symbols_keyboards"
"settings_key_use_backword" : "settings_key_use_backword"
"settings_key_use_contacts_dictionary" : "settings_key_use_contacts_dictionary"

POSSIBLE SECRETS

"settings_key_use_custom_sound_volume" : "use_custom_sound_volume"

"settings_key_use_key_repeat" : "use_keyrepeat"

"settings_key_use_user_dictionary" : "settings_key_use_user_dictionary"

"settings_key_use_volume_key_for_left_right" : "settings_key_use_volume_key_for_left_right"

"settings_key_vibrate_on_key_press_duration_int" : "settings_key_vibrate_on_key_press_duration_int"

"settings_key_vibrate_on_long_press" : "settings_key_vibrate_on_long_press"

"settings_key_workaround_disable_rtl_fix" : "settings_key_workaround_disable_rtl_fix"

"tweaks_group_key" : "tweaks"

"user_dict_editor_key" : "user_dict_editor_key"

394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731112316

50934d3e385b490c882f0e756e14855d

1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

b869c82b35d70e1b1ff91b28e37a62ecdc34409b

fJzM8V+ATbwMqso1FfvPLoBhYN4ojhn6bStsV+iGZGXUcAQ5UdVWi/JBwFYSjW+Z

767d9b01105c2acd25fb7955a5394f78

POSSIBLE SECRETS

8k8YzM5wR7o+JxVSif6W3gUExnUXRa+1SaNfeXoc/KI=

E49D5C2C0E11B3B1B96CA56C6DE2A14EC7DAB5CCC3B5F300D03E5B4DBA44F539

3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

32670510020758816978083085130507043184471273380659243275938904335757337482424

nPgtvuonjnkWdghv0SijHg6/i9Y34D7EpYJU2u9rcQe20YVAO3kNDyZXdnFoabyE

115792089210356248762697446949407573529996955224135760342422259061068512044369

5YZBRBaKVoc53PJNiLp/sxiQ4sgkDdqNOlYuo9Kj11A=

42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76
137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586
d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b
035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a

173cf86fe9894a0f70dadd09d4fd88c380836099d4939f8c3754361bdc16a32b

115792089210356248762697446949407573530086143415290314195533631308867097853951

r8lambdaXeEi0T5Vz7e8r3qvWmqYHfELP4

115792089237316195423570985008687907853269984665640564039457584007908834671663

962eddcc369cba8ebb260ee6b6a126d9346e38c5

POSSIBLE SECRETS

308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d010104050030819431 0b3009060355040613025553311330110603550408130a436 16c69666f726e69613116301406035504070713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f696431 10300e060355040b1307416e64726f69 43110300e06035504031307416e64726f696431 22302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d303830343135323333 3635365a170d33353039303031323333333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504070713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312 2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d0030820108028201010 0d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a 92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4d d9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87d d3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e04160414 8d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009 06035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504070713 0d4d6f756e7461696e20566965773110300e060355040a1307416e6 4726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696431 22302006092a864886f70d0109011613616e64726f696440616e6 4726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d010104050003820101 0019d30cf105fb78923f4c0d7dd223233 d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e6181 86673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c196 2fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb 21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

sha256/eIsBT7ALukWdTzVOIpNEJ7d29IKTHYKTMWTFQyhzYSs=

2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846

CMP58KUFBRi55MrO79QJf+iIcc+kMldspC1nSaWllCQ=

NEFdqqAAKqlTQEHTml6xaqDgpQZyg1pRnKumbN+eqhQCHZmsI8VG5KhrQKR43pSu

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

1Cs3HyJ4gdHs1TY1t1mRXKXwLGuIk9WztHFAT7PZCzg=

0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78

POSSIBLE SECRETS

6HNxGbhhczkgMwux7c1JnxuvU0wUTaRoejYXAQva8ckSWURuEsC3usSfONdhI0SW

89jQARCIO27CLJ3vyAIPxf7eWUDAKRbGk8uiXj6moxg=

80fedfd8941a368fafdae46750a4d367

308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b300906035504061302555331133011060355040813 0a4361 6c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d30383038323133233313333345a170d333630313037323331333334345a3074310b3009060355040613025 5533113301106035504081 30a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965657731143012060355040a130b476f6f676c6520496e632e e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b300906035504061302555331133011060355040813 0a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a

f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc

9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511

44x6GMcLLfXIM1YaNbXK6PVfUUKLz6aX2MRhfiwtXAQ=

db48223fd9e143f7e133c57f5d08a4e38549ce3ebd921fe3b4003c26e5e35bed

POSSIBLE SECRETS

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

65799ed4c04eaa0011e94930

9b8f518b086098de3d77736f9458a3d2f6f95a37

f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773

db53fcdc9ab71e9bdd4eab257fe1aba7989ad2b24fbe3a85dfef72ea1dd6bae2

d80f18e8081b624cc64985f87f70118f1702985d2e10dbc985ee7be334fd3c7d

e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe
9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf

3Va0stlf242U1Ue7o9TlJnm/36RIQrt1QqEOlEimTMw=

3517262215D8D3008CBF888750B6418EDC4D562AC33ED6874E0D73ABA667BC3C

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

EqhZfeJdagDkdmNpQFhVQ7G0RKq67vK3QlT8DoNCRs8=

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505714

POSSIBLE SECRETS

a14a2bf76d12e8b79a9bc6

l7Z8iinoDf65D6f8x6SJHqGD1Z2cIloE56napHJ3hKPe1zHuuQTwZLhUlKl9SuDr

e2f856b9f9a4fd4cb2795aeaf83268e4bff189aaec05d691ffde76e075b82648

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

rj4PFJqgmPTylFXY08pNaAuPZORxwcZUguOBeXhMFKg9NNv3

2LHYpyDYp9mG2KrYrtin2Kgg2qnZhtuM2K8g24zaqSDZgdin24zZhA==

2KfbjNqpINmB2KfYptmEINmF24zauiDYs9uSINin2YbYqtiu2KfYqCDaqdix24zaug==

410583637251521421293261297800472684091144410159937255548352563140 39467401291

2A57086C86EF54970C1E6EB37BFC72B1

83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473 33078086511627871

e9702f1e92e97fce49cdf81a5fa730a4e913554d09b3fe41e1d8a7fba00a8459

fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

MvgiGujNJnCbH7w8ay+vn+9KOY0pB5PpnwUR2iVU8Do=

POSSIBLE SECRETS

484395612939064517590525852527979142027629495260417479958440807171708240 4635286

678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

Iq9SbqSJ8yU7RzOiISCe3nCpBjH6mJ670ZCopYguBesKZiSJJGgYhB6NljSGo9ir

403f14ad2f0e5eb3c4f3a0bcd5c1592cc4492662ad53191c92905255d4990656

E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

065c917c19b181c637c50d86a36be654

7ZWY64KY7J2YIO2MjOydvOydhCDshKDtg50=

7f2189aefbaf801f6ce08055c95d152b389fe187

5fed96c85bd58c58aadbd465c172a4c9a794d8eb2f86cbc7bcee6caf4c7a2c5f

3081a0adab3018d57165e6dd24074bdbac640f6dbe21a9e24d3474a87ebf38b8

b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536

24fbae40bcd50b759b26e3ba0f46aa25e932fa7da05f226d75ec507bcf53bce5

POSSIBLE SECRETS

470fa2b4ae81cd56ecbcda9735803434cec591fa

c56fb7d591ba6704df047fd98f535372fea00211

30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c1585
47f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252

f8d927750a0952ffb5bd87dfb83d781ae65f7bed043a7886d1d3cdcfc94bb77a

cc2751449a350f668590264ed76692694a80308a

B92825C2BD5D6D6D1E7F39EECD17843B7D9016F611136B75441BC6F4D3F00F05

70b60dd321d4b83d596f4f9e6a24f10b

f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5
47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

UrVBgf9243jndsa9S6xVT15cQBp

27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

755UReg2OebscDfMisTRcyHgU7deIoPFggCY/cxxLVcYt5+XFw3QcrbbBvUI25X2

394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336653942643

O/RWom2ttXKsxcIeQt9LD0kGEjz6kElPF5Gfn2k8dvND1rDfknl9Z31RPOB5g0G+

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS

26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

2ehMwY4NjAVCxKNUUqdAHAq3dStVMVXOFsI0kFp0ZW0=

4bdecdf772491e35c4e8b48f88aee22bae1311984f2e1da4dfad0b78ee7f5163

b368b110e3b565fe97c91f786e11bc48754cc8e4e6f21d8a94a68ac6ad67aaaf

FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

9760508f15230bccb292b982a2eb840bf0581cf5

AIzaSyAfFWdgvoxxTuOB6xvaNpuO6G299R5pcCQ

F5L8q737MMzYnugLKIPW4LyN3bjV9SheOjBtsYe5lqc=

o47UOqvH2XIjJOSYtJICa4qB9IxNnqh6Nq71y7pdPyU=

4230baa077b401374d0fc012375047e79ea0790d58d095ef18d97d95470c738d

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

DPPujNohd+oH/T6ZUMbZzyhfnSIvMDgRP7rWCRWsFdFXxrCKVlDjhvyLuEdzf2o9

POSSIBLE SECRETS

aOe/514coVpPRQegN4yl3ZJgMMZH4bY8vGVrQ08DnDuyKsRCp48F+Zjpb0HjBNAa

375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434 4277578376784

92974c6802419e4d18b5ec536cbfa167b8e8eff09ec4c8510a5b95750b1e0c82

1157920892373161954235709850086879078528375642790749043826051631415181614943 37

07ff9b7aeeff969173c45b285fe0fecdbaae244576ff7a2796a36f1c0c11adb4

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

RsQqTTopQSSPcEVMkYGLNYEBC1gHD99rtwIfq5A0FgY=

YKKxGLeU2zJMORJ3CXggTVER1rcusEu7lPKzdwQPcOhmeA2WpnQ11LfNiSgl6FV6

77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399

8d5155894229d5e689ee01e6018a237e2cae64cd

9a04f079-9840-4286-ab92-e65be0885f95

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

1157920892103562487626974469494075735300861434152903141955336313088670978539 48

POSSIBLE SECRETS

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

c103703e120ae8cc73c9248622f3cd1e

49f946663a8deb7054212b8adda248c6

85053bf24bba75239b16a601d9387e17

GPnS+VgCUEsE+Z+TtHFvZYB0s31DHdUZ2eNJil33wtg=

CL5CLQrzdJf7Vwsm6HGAxqUk+UMWsbN6k++UR113AdLOMpqSaLq8guKKFWwu33sx

B3EEABB8EE11C2BE770B684D95219ECB

36134250956749795798585127919587881956611106672985015071877198253568414405109

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

30820122300d06092a864886f70d01010105000382010f003082010a0282010100a3d269348ac59923f65e8111c337605e29a1d1bc54fa96c1445050dd14d8d63b10f9f0230bb87ef348183660bedcabfdec045e235ed96935799fcdb4af5c97717ff3b0954eaf1b723225b3a00f81cbd67ce6dc5a4c07f7741ad3bf1913a480c6e267ab1740f409edd2dc33c8b718a8e30e56d9a93f321723c1d0c9ea62115f996812ceef186954595e39a19b74245542c407f7dddb1d12e6eedcfc0bd7cd945ef7255ad0fc9e796258e0fb5e52a23013d15033a32b4071b65f3f924ae5c5761e22327b4d2ae60f4158a5eb15565ba079de29b81540f5fbb3be101a95357f367fc661d797074ff3826950029c52223e4594673a24a334cae62d63b838ba3df9770203010001

t8m4GxfDNdbzfvzmJ7ERdURqh0DgV49Pg4cGI5qmXbo=

f4596eeb-7ff5-4a25-83d4-4b423a6e4267

POSSIBLE SECRETS

3ti3ezo40ryM1w4gfDBvjiqMuHkyKLnrJqm+zFKeNdY=

xrMIVw+CZrXn1IekizTiUScI6wNAILuxj1b/rhxDE2pwil0Ht31LBwVl9aHUCekb

3AJSAiPIa+BfzMb1UB6dOa0g/yKIYU+RvBwyuDyaJrc=

kypbHNkssvP0JsUhutxcI0i2X1rFBFEIMdtXVFZfH9yzsagSauN+Hc+hylkiTIg3

5506626302227734366957871889516853432625060345377759417550018736038 9116729240

3940200619639447921227904010014361380507973927046544666794829340424572177 1496870329047266088258938001861606973112319

vwafhzajmko+XbfuSejKABEanPVybMYr0Xs0X58XDfD46RrNvhHs28KurUcFj7Vb

F65Z/VGvH3HDSqbisIa05H0FMwZRHR3bv6841vtkw2aGLMzg81raAO8ZiFdKkdju

Q7CPoNnCWDIIOccltii1S+O+2a/ZVRW78C0n4S9Y84k=

Vzvp2EkF2pEbKPIdCn3PFXroHmxxEvOZYSjqA8kd9hBeO5S3wxnRIFg589Z0eHEB

39b0c69faa2679eeb0d545

4aec669e-ca07-4d5a-943c-f29e0c337ed4

LyfKIPN68aZRbmvxI0qKlkb7QqDxcBxbJuROIg+7WFc=

TWYb54U7OgagGMZWjzU5K3jAzzOExDb/MqAF9pfakrM=

▷ PLAYSTORE INFORMATION

Title: JazzCash - Your Mobile Account

Score: 4.4773793 **Installs:** 50,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.techlogix.mobilinkcustomer

Developer Details: Jazz Pakistan - Official, Jazz+Pakistan+-+Official, Jazz Digital Headquarters Kohistan Road, F8 Markaz, Islamabad Pakistan, https://www.jazzcash.com.pk, jazzcashappfeedback@jazz.com.pk,

Release Date: Jul 17, 2016 **Privacy Policy:** Privacy link

Description:

Welcome to JazzCash, Pakistan's largest fintech app. With seamless mobile money services, JazzCash revolutionises how you handle your finances. It is your go-to app for all your financial needs, offering features from QR payments to online banking. JazzCash offers the ultimate mobile wallet experience, combining convenience, security, and a range of features. A Complete Suite of Mobile Wallet Services JazzCash provides a comprehensive mobile wallet solution, making managing your money on the go easier than ever. Whether you're looking to transfer money to a friend, pay your bills, or load your mobile phone, JazzCash has got you covered. As Pakistan's number one wallet, we offer unparalleled convenience and security. Money Transfer With our user-friendly app, you can send money instantly to friends and family. You can also quickly and securely transfer money to any bank account in Pakistan. With just a few taps, you can pay anyone, anywhere, anytime. QR Payments Forget carrying cash. With JazzCash, you can make instant QR payments at thousands of merchants nationwide. Just scan and pay – it's that simple! Enjoy a cashless shopping experience with our reliable and swift payment system. Loans & Savings Need a little extra cash? JazzCash offers quick and easy loans directly through the app. Plus, you can grow your savings with our savings accounts. Manage your finances smartly and securely with JazzCash. Debit Cards JazzCash provides you with the convenience of a debit card for online and in-store purchases. Enjoy the flexibility of using your funds anywhere, anytime. Our debit cards are linked directly to your mobile wallet, ensuring your money is always within reach. Online Payments Make online payments effortlessly with JazzCash. Whether you're shopping online, booking tickets, or subscribing to services, our app ensures smooth and secure transactions. Say goodbye to complicated payment processes and hello to ease and convenience. Government Payments JazzCash allows you to pay a range of government payments for the Federal Board of Revenue (FBR), NADRA, Punjab Revenue Authority, Government of Punjab Excise and Taxation, Islamabad Vehicle Token Tax, Government of Sindh Vehicle Token Tax, traffic challans and online machine-readable passport renewal fees. Education Payments Paying for school fees has never been easier. With JazzCash, you can pay education-related expenses directly from your mobile wallet. Ensure your education payments are always on time and hassle-free. Insurance Protect yourself and your loved ones with JazzCash's insurance services. Easily purchase and manage your health and life insurance through the app at minimal rates, ensuring peace of mind at your fingertips. Offers, Loyalty Programs, Cashbacks & Discounts JazzCash rewards your loyalty with exciting offers, cashback deals, and exclusive discounts. Stay tuned to our app for the latest promotions and make the most out of your spending. Save more every time you use JazzCash for your payments. Unmatched Security & Instant Payments Your security is our priority. JazzCash uses state-of-the-art encryption and security measures to protect your transactions and personal information. Enjoy peace of mind with our instant payments and secure money transfer services. Download JazzCash now and take control of your finances with Pakistan's most trusted mobile wallet. Experience the future of money management today!

≔ SCAN LOGS

Timestamp	Event	Error

2024-10-19 10:48:18	Generating Hashes	OK
2024-10-19 10:48:18	Extracting APK	OK
2024-10-19 10:48:18	Unzipping	OK
2024-10-19 10:48:20	Getting Hardcoded Certificates/Keystores	OK
2024-10-19 10:48:27	Parsing AndroidManifest.xml	OK
2024-10-19 10:48:27	Parsing APK with androguard	OK
2024-10-19 10:48:28	Extracting Manifest Data	OK
2024-10-19 10:48:28	Performing Static Analysis on: JazzCash (com.techlogix.mobilinkcustomer)	OK
2024-10-19 10:48:28	Fetching Details from Play Store: com.techlogix.mobilinkcustomer	OK
2024-10-19 10:48:29	Manifest Analysis Started	OK
2024-10-19 10:48:31	Reading Network Security config from network_security_config.xml	OK

2024-10-19 10:48:31	Parsing Network Security config	OK
2024-10-19 10:48:31	Checking for Malware Permissions	OK
2024-10-19 10:48:31	Fetching icon path	OK
2024-10-19 10:48:31	Library Binary Analysis Started	OK
2024-10-19 10:48:31	Reading Code Signing Certificate	OK
2024-10-19 10:48:33	Running APKiD 2.1.5	OK
2024-10-19 10:48:43	Detecting Trackers	OK
2024-10-19 10:48:50	Decompiling APK to Java with jadx	OK
2024-10-19 11:04:09	Converting DEX to Smali	OK
2024-10-19 11:04:09	Code Analysis Started on - java_source	OK

2024-10-19 11:15:01	Android SAST Completed	OK
2024-10-19 11:15:01	Android API Analysis Started	OK
2024-10-19 11:26:31	Android Permission Mapping Started	OK
2024-10-19 11:37:27	Android Permission Mapping Completed	OK
2024-10-19 11:37:54	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 11:37:54	Extracting String data from APK	OK
2024-10-19 11:37:54	Extracting String data from Code	OK
2024-10-19 11:37:54	Extracting String values and entropies from Code	OK
2024-10-19 11:38:09	Performing Malware check on extracted domains	OK
2024-10-19 11:38:24	Saving to Database	OK

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.