APP SCORES

Security Score

58/100

Trackers Detection

2/432

FILE INFORMATION

File Name Emkay Blitz.apk

Size 7.27MB

MD5 e3e6b72da8630e44c59ed7bdf8c834dd

SHA1 cee4bfb8b99465fdecaa828da3e9147e1ebffdbd

SHA256

dc45afc36511a1fe7178b8c609393f554f3688ae0eddef1992601a4d198c7951

APP INFORMATION

App Name Emkay Blitz

Package Name

com.emkayglobal.emkayblitz

Main Activity

com.emkayglobal.emkayblitz.MainActivity

Target SDK 34 **Min SDK** 26 **Max SDK**

Android Version Name 1.0.8

Android Version Code 109

PLAYSTORE INFORMATION

Title Emkay Blitz

Score None **Installs** 1,000+ **Price** 0 **Android Version Support** **Category** Finance **Play Store URL** com.emkayglobal.emkayblitz

Developer Emkay Global Financial Services Ltd., **Developer ID** Emkay+Global+Financial+Services+Ltd.

Developer Address None

Developer Website https://www.emkayglobal.com/

Developer Email itsupport@emkayglobal.com

Release Date Jan 2, 2023 **Privacy Policy** Privacy link

Description

```
Emkay Blitz brings the stock market to your mobile phone through this easy-to-use app, with lots of
interesting add-ons and convenient features that you'll absolutely love. You'll get addicted before
you know it!

 * Get real-time stock quotes and solid industry tips
 * Trade and track in equity, commodity, currency and F&O

Transfer funds online
Emkay Blitz is a unique online trading platform, which offers stock broking services at flat rates
with the added benefits of expert research and analysis. Flat pricing offers you great savings over
the traditional percentage model.
This app brings all the benefits of Emkay Blitz to your mobile phone – so you can trade conveniently
on the go, anytime.

1. Member name: Emkay Global Financial Services Limited
2. SEBI Registration Number`: INZ000203933
3. Member Code: 9018, 185, 56270, 1263, 1089
4. Registered Exchange/s name: NSE, BSE, MCX, NCDEX, MSEI
5. Exchange approved segment/s: Cash, F&O, CD, Commodity , IRF, SLBM, MFSS
```

18	10	8	5
ACTIVITIES	SERVICES	RECEIVERS	PROVIDERS
View	View	View	View
Exported	Exported	Exported	Exported

Activities
0

Services
1

Receivers
2

Providers
0

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-01-02 09:31:18+00:00
Valid To: 2053-01-02 09:31:18+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6b0692eb0277eb092257940b5f82875ebc8503da
Hash Algorithm: sha256
md5: 3b4e410abbce674b36b6d1c0de01db0e
sha1: c588c3ae5ac47be6a5c4f39fd5cb5978e1238a26
sha256: 1b55bfa9edfef59a2aadccf789449dd4da760229a35a40db259173844d8b6184
sha512:
267d5ababd6408c9d4a5d2eb57202deb44d1ca41f3fce0a33245b360a0ffbe8d88e5124a913cb092ae0a5a994c5bbfda405ea
8c634c2e17a3c0f827246fa6b1f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: dab2172e12fa4b2fed0fb23b1313fe0f87bc82fed12fa1bc2ccb35e6065f5008
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications	
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.	
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.	
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	CODE MAPPINGS
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.	

Showing 1 to 10 of 17 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	

API	FILES
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Execute OS Command	
Get Installed Applications	
Get Phone Number	

Showing 1 to 10 of 35 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	0	0	1

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.

Showing 1 to 1 of 1 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO

0	0	1

Search:

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

Showing 1 to 1 of 1 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
0	4	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

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

NO	ISSUE	SEVERITY	DESCRIPTION
3	**Broadcast Receiver** (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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

NO	ISSUE	SEVERITY	DESCRIPTION
			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
4	**Broadcast Receiver** (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal

NO	ISSUE	SEVERITY	DESCRIPTION
			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
5	**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

NO	ISSUE	SEVERITY	DESCRIPTION
			malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

Showing 1 to 5 of 5 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	9	2	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	The App logs information. Sensitive information should never be logged.	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3		
2	The App uses 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	c9/a.java j8/k.java k9/h.java	
3	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	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/cashfree/pg/core/api/ui/BaseCFWebView.java	
5	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		
6	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
7	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		
8	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		
9	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
10	This App may request root (Super User) privileges.	warning	**CWE:** CWE-250: Execution with Unnecessary Privileges **OWASP MASVS:** MSTG-RESILIENCE-1	m9/a.java	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

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

Showing 0 to 0 of 0 entries

Previous Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Hardcoded Keystore found.	assets/grs_sp.bks assets/hmsincas.bks assets/hmsrootcas.bks

Showing 1 to 1 of 1 entries

Previous 1 Next

APKiD ANALYSIS

Search:

DEX	DETECTIONS

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check subscriber ID check possible ro.secure check
Compiler	unknown (please file detection issue!)

Showing 1 to 3 of 3 entries

Previous 1 Next

Showing 1 to 1 of 1 entries

Previous 1 Next

QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

ABUSED PERMISSIONS

Top Malware Permissions **7**/24

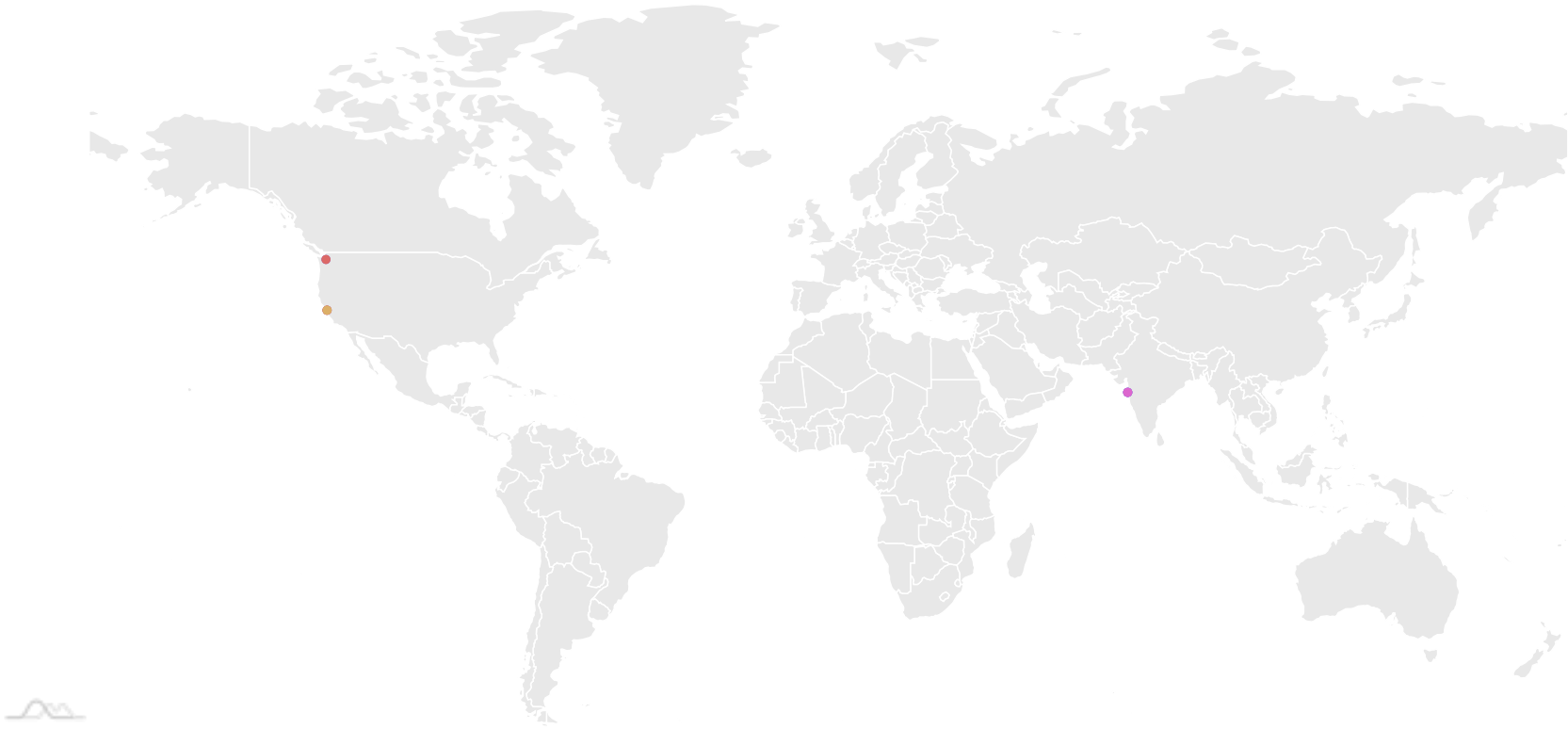
android.permission.INTERNET,
android.permission.WAKE_LOCK,
android.permission.ACCESS_NETWORK_STATE,
android.permission.RECEIVE_BOOT_COMPLETED,
android.permission.VIBRATE,
android.permission.ACCESS_FINE_LOCATION,
android.permission.ACCESS_COARSE_LOCATION

Other Common Permissions

com.google.android.c2dm.permission.RECEIVE,
com.google.android.gms.permission.AD_ID,
com.google.android.finsky.permission.BIND_GET_INSTALL_REFE

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

SERVER LOCATIONS



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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 64.233.170.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.cashfree.com	ok	**IP:** 13.126.9.35 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
cashfreelogo.cashfree.com	ok	**IP:** 13.227.138.88 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.67.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.250.192.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
payments-test.cashfree.com	ok	**IP:** 13.126.10.96 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
payments.cashfree.com	ok	**IP:** 65.1.7.204 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.76.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	ok	**IP:** 142.250.182.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
receiver.cashfree.com	ok	**IP:** 13.234.155.102 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map

Showing 1 to 10 of 13 entries

Previous 1 2 Next

URLS

Search:

URL	FILE
data:!0}),_t=function(){return	com/pichillilorenzo/flutter_inappwebview/plugin_scripts_js/PromisePolyfillJS.java
file:///android_asset/	com/pichillilorenzo/flutter_inappwebview/Util.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java
https://%s/%s/%s	r7/c.java
https://accounts.google.com/o/oauth2/revoke?token=	v3/f.java
https://api.cashfree.com/pg/orders/pay/authenticate/ https://sandbox.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeResendOTPRequest.java
https://api.cashfree.com/pg/orders/pay/authenticate/ https://sandbox.cashfree.com/pg/orders/pay/authenticate/	com/cashfree/pg/core/hidden/network/request/NativeSubmitOTPRequest.java

URL	FILE
https://api.cashfree.com/pg/orders/sessions/app https://sandbox.cashfree.com/pg/orders/sessions/app	com/cashfree/pg/core/hidden/network/request/BaseNetworkRequest.java
https://cashfreelogo.cashfree.com/assets_images/pg/nb/%s%s.png	l2/b.java
https://cashfreelogo.cashfree.com/assets_images/pg/paylater/%s%s.png	l2/g.java

Showing 1 to 10 of 27 entries

Previous 1 2 3 Next

FIREBASE DATABASE

EMAILS

Search:

EMAIL	FILE
u0013android@android.com u0013android@android.com0	y3/w.java

Showing 1 to 1 of 1 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

Showing 1 to 2 of 2 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▸ Show all **329** secrets

STRINGS

From APK Resource

▶ Show all **226** strings

From Code

▶ Show all **12762** strings

From Shared Objects

ACTIVITIES

▼ Showing all **18** activities

com.emkayglobal.emkayblitz.MainActivity
com.pichillilorenzo.flutter_inappwebview.in_app_browser.InAppBrowserActivity
com.pichillilorenzo.flutter_inappwebview.chrome_custom_tabs.ChromeCustomTabsActivity
com.pichillilorenzo.flutter_inappwebview.chrome_custom_tabs.TrustedWebActivity
com.pichillilorenzo.flutter_inappwebview.chrome_custom_tabs.ChromeCustomTabsActivitySingleInstance
com.pichillilorenzo.flutter_inappwebview.chrome_custom_tabs.TrustedWebActivitySingleInstance
io.flutter.plugins.urllauncher.WebViewActivity
com.wongpiwat.trust_location.TrustLocationPlugin
com.cashfree.pg.ui.hidden.checkout.CashfreeNativeCheckoutActivity
com.cashfree.pg.ui.hidden.seamless.CFDropSeamlessActivity
com.cashfree.pg.core.api.ui.CFCoreUPIPaymentActivity
com.cashfree.pg.core.api.ui.CFCoreModalActivity
com.cashfree.pg.core.api.ui.CashfreeCoreNativeVerificationActivity
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
com.google.android.gms.common.api.GoogleApiActivity

com.google.android.play.core.common.PlayCoreDialogWrapperActivity
com.huawei.hms.activity.BridgeActivity
com.huawei.hms.activity.EnableServiceActivity

SERVICES

▼ Showing all **10** services
io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingBackgroundService
io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.messaging.FirebaseMessagingService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.huawei.agconnect.core.ServiceDiscovery

RECEIVERS

▼ Showing all **8** receivers
io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver
com.dexterous.flutterlocalnotifications.ActionBroadcastReceiver
com.dexterous.flutterlocalnotifications.ScheduledNotificationReceiver

com.dexterous.flutterlocalnotifications.ScheduledNotificationBootReceiver
com.pichillilorenzo.flutter_inappwebview.chrome_custom_tabs.ActionBroadcastReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

PROVIDERS

▼ Showing all **5** providers
io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingInitProvider
com.cashfree.pg.api.CashfreeCoreContentProvider
com.google.firebase.provider.FirebaseInitProvider
androidx.startup.InitializationProvider
com.huawei.agconnect.core.provider.AGConnectInitializeProvider

LIBRARIES

▼ Showing all **2** libraries
androidx.window.extensions
androidx.window.sidecar

FILES

► Show all **804** files

 Version v4.0.7