ANDROID STATIC ANALYSIS REPORT

AmigoExpress (1.8.1)

File Name:	amigo-base.apk
Package Name:	com.amigoexpress.android
Scan Date:	Nov. 28, 2025, 1:11 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	3	3	1

FILE INFORMATION

File Name: amigo-base.apk
Size: 12.15MB
MD5: c82f3ceebcebe7dbe394e8d856935383
SHA1: b9d0522a11a8a5eaaeec638f0206123d0ca63b9e
SHA256: 6a3185850e2a9eb6db3391382b7a72bdfc64fa72bf530d03745552abdcb6a4da

APP INFORMATION

App Name: AmigoExpress
Package Name: com.amigoexpress.android
Main Activity: com.amigoexpress.android.controller.home.SplashScreen
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 1.8.1

Android Version Code: 260

APP COMPONENTS

Activities: 103
Services: 8
Receivers: 4
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-02 20:17:50+00:00
Valid To: 2049-08-02 20:17:50+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x36166fc1b428ed81e2e94a10e02142518d9261e5
Hash Algorithm: sha256
md5: 4d92a391a12561a2b113c950d139e7e6
sha1: 33ce9d12556b9ad147777a2d4948a0c35bf2c8b0
sha256: 687aa965829c49d1c04bc04b7b8fd98b1c53abfecc7f3f69860bddf002bf6888
sha512: 2c25f9e4d4c4ec4489c7ca4f358b9ca01b5abe945aacac326fc60a6fd23ba3e04340a8fd768ff962fe299053f878e39910f57f87988f8555b38ecd09ab968e44
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 447515c45575008ae389aa5552db8d1dd06cdc320ba23569381e8fd70d8d0f72
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.amigoexpress.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.

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: **1** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched 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.

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.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a 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.
5	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

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/h.java A2/b.java A2/c.java A2/j.java A2/l.java A2/n.java A5/a.java A5/h.java B/c.java B/r.java B1/e.java C2/d.java C2/w.java C2/y.java C2/z.java C5/c.java C5/d.java D/d.java D/i.java D/j.java D/m.java D/q.java D3/A.java D3/B.java D3/C0025b.java D3/C0033d1.java D3/C0044h0.java D3/C0053k0.java D3/C0096z.java D3/RunnableC0032d0.java D3/RunnableC0083u1.java D3/RunnableC0085v0.java D3/RunnableC0094y0.java D3/U0.java D3/X1.java D3/Y.java D3/d2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				D5/a.java D5/b.java D5/c.java D5/f.java E1/k.java E5/b.java E5/c.java E5/d.java E5/f.java E5/k.java E5/q.java F/g.java F0/C0111m.java F2/h.java G0/e.java G0/q.java G2/e.java G3/a.java G4/d.java G4/g.java H/AbstractC0125h.java H/C.java H/C0123f.java H/RunnableC0118a.java I/g.java I1/c.java I4/a.java I5/C0167o.java I5/C0168p.java I5/C0169q.java I5/C0172u.java I5/E.java I5/I.java I5/P.java I5/S.java I5/W.java I5/X.java I5/Z.java I5/a0.java I5/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				J0/j.java J3/d.java J4/a.java J4/b.java J4/c.java K/b.java K/m.java L/d.java L/f.java L/g.java L/h.java L/i.java L/j.java L/l.java L4/b.java M/e.java M4/A.java M4/B.java M4/g.java M4/h.java M4/k.java M4/m.java M4/o.java M4/s.java M4/t.java M4/u.java M4/v.java M4/x.java M5/c.java M5/d.java M5/e.java N2/s.java N4/e.java O3/n.java O4/e.java O4/h.java O4/m.java O4/o.java O4/p.java P3/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Q/k.java Q0/e.java R/a.java R/d.java R/m.java R0/a.java R3/a.java R3/c.java R6/M.java S4/a.java S4/c.java T0/c.java T0/g.java T0/h.java T0/l.java T4/c.java U0/a.java U0/f.java U2/d.java U2/i.java V/C0284b.java V/M.java V/W.java V/X.java V/l0.java V/m0.java V/r.java V/r0.java W0/a.java Y/k.java Y1/a.java Z2/b.java Z2/c.java a/AbstractC0317a.java a7/d.java a7/l.java a7/n.java b0/d.java b4/b.java b4/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive	b6/C0489b.java b7/e.java c3/b.java c3/d.java c3/e.java c3/f.java c3/i.java c3/j.java c3/k.java c3/l.java c6/a.java c6/e.java c6/h.java c6/i.java c6/q.java c6/r.java com/amigoexpress/android/controller/home/filters/alert/AlertMessageActivity.java com/amigoexpress/android/controller/home/filters/commitment/CommitmentActivity.java com/amigoexpress/android/controller/home/filters/friends/FriendsActivity.java com/amigoexpress/android/controller/home/filters/invalidePlacePoint/EditInvalidePlaceActivity.java com/amigoexpress/android/controller/home/filters/missinginfo/MissingInfoActivity.java com/amigoexpress/android/controller/home/filters/suspended/SuspendedActivity.java com/amigoexpress/android/controller/home/filters/transnational/TransnationalActivity.java com/amigoexpress/android/controller/home/filters/update/MandatoryUpdateActivity.java com/amigoexpress/android/controller/home/pager/announce/start/search/SearchPickupPointsActivity.java com/amigoexpress/android/controller/home/pager/announce/start/usualAnnounce/UsualAnnounceTimeActivity.java com/amigoexpress/android/controller/home/pager/announce/start/verification/intermediate/stop/Delet

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	eIntermediateStopActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingAddReservationActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingCancelActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingCancelDefaultActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingCarActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingDriverActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingLocationActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingPassengerActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingPaymentInfoActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RideCancelActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RidePassengerActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/intermediate/SearchIntermediateCityActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/intermediate/price/RideAddIntermediateStopPricesActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/intermediate/price/RideEditIntermediateStopPricesActivity.java com/amigoexpress/android/controller/home/pager/profile/settings/SettingsActivity.java com/amigoexpress/android/controller/home/pager/profile/settings/verifyphone/VerifyPhoneActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amigoexpress/android/controller/home/pager/search/filters/SearchDateWeekActivity.java com/amigoexpress/android/controller/home/pager/search/itinerary/ItineraryCarActivity.java com/amigoexpress/android/controller/home/pager/search/itinerary/ItineraryDriverActivity.java com/amigoexpress/android/controller/home/pager/search/itinerary/ItineraryIntermediateCitiesActivity.java com/amigoexpress/android/controller/home/pager/search/itinerary/SearchItineraryActivity.java com/amigoexpress/android/controller/home/pager/search/places/SearchPlacesActivity.java com/amigoexpress/android/controller/home/support/WebViewActivity.java com/amigoexpress/android/controller/view/AENestedScrollView.java com/amigoexpress/android/controller/view/AEScrollView.java com/amigoexpress/android/controller/view/AEViewCategory.java com/amigoexpress/android/controller/view/AEViewPager.java com/amigoexpress/android/model/api/base/AEBaseSerializer.java com/amigoexpress/android/model/api/search/ApiSearchFilter.java com/amigoexpress/android/model/content/AEContentDisplay.java com/amigoexpress/android/model/content/JsonObjectParcelConverter.java com/amigoexpress/android/model/requests/RequestSearchItineraries.java com/amigoexpress/android/model/responses/base/AEBaseResponse.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/d.java com/bumptech/glide/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/k.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/m.java com/livechatinc/inappchat/ChatWindowViewImpl.java d3/AbstractBinderC0705m.java d3/AbstractC0699g.java d3/AbstractC0708p.java d3/C0697e.java d3/C0700h.java d3/HandlerC0702j.java e/i.java e2/C0722b.java e4/d.java e6/ViewOnFocusChangeListenerC0738b.java f2/j.java f3/C0766d.java f3/l.java f3/m.java f3/p.java f3/u.java f4/AbstractC0772d.java g2/q.java g3/AbstractC0800e.java g3/C0803h.java g3/C0811p.java g3/D.java g3/E.java g3/G.java g3/J.java g3/L.java g3/s.java g3/t.java h/AbstractActivityC0858l.java h/AbstractC0864r.java h/C0828A.java h/C0866t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h/LayoutInflaterFactory2C0832E.java h4/C0884e.java h4/C0886g.java i5/C0922b.java j1/C1130e.java j2/C1135e.java j2/q.java j3/C1145a.java j5/C1151c.java k1/AbstractActivityC1162b.java k2/C1166c.java k3/AbstractC1170b.java k3/AbstractC1172d.java l0/C1199b.java l0/C1200c.java l0/g.java l2/C1209c.java l2/C1210d.java m/h.java m/i.java m2/C1225a.java m3/AbstractC1228a.java n/f.java n/l.java n0/AbstractC1267c.java n3/f.java n5/A.java n5/d.java n5/f.java n5/h.java n5/k.java n5/p.java n5/q.java n5/r.java n5/u.java n5/v.java n5/w.java n5/y.java o/A0.java o/C1293c0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/C1325t.java o/E0.java o/G.java o/H0.java o/I0.java o/M0.java o/O0.java o/Y.java o/c1.java o/r.java o2/C1345b.java o3/AbstractC1353f.java o3/C1351d.java p2/C1369B.java p2/k.java p2/l.java p2/n.java q1/C1399d.java q2/f.java q2/g.java q4/c.java q5/C1409b.java r2/C1418c.java s/C1431C.java s/g.java s/m.java s/z.java t0/y.java t2/C1478b.java t2/C1479c.java t2/C1480d.java u5/C1527a.java v2/C1547c.java w2/C1562b.java w2/F.java w2/h.java w2/l.java w2/p.java w2/r.java w2/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	A5/e.java C2/d.java C4/a.java D3/d2.java D5/g.java D5/h.java D5/i.java E1/n.java E5/c.java E5/n.java E5/q.java j$/util/concurrent/ThreadLocalRandom.java
3	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	H5/c.java O4/b.java P4/C0204f0.java com/amigoexpress/android/model/api/login/ApiLogin.java com/amigoexpress/android/model/api/login/ApiLoginRefresh.java n2/C1277i.java p2/C1368A.java p2/C1373d.java p2/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	D3/C0061n.java D3/M0.java D3/P.java D3/RunnableC0094y0.java D3/X1.java D3/Z.java D5/b.java E5/i.java E5/k.java H4/b.java Q5/c.java U2/d.java U2/i.java V2/j.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	a7/e.java a7/h.java a7/m.java a7/n.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	M4/h.java R6/M.java i5/C0922b.java k3/AbstractC1170b.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	c6/i.java g3/C0811p.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/livechatinc/inappchat/ChatWindowViewImpl.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	M4/h.java q4/e.java
10	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	A2/c.java
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	t0/ViewOnCreateContextMenuListenerC1464k.java
12	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	D3/d2.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	O4/h.java g3/C0811p.java
00022	Open a file from given absolute path of the file	file	O4/h.java
00013	Read file and put it into a stream	file	D5/f.java H/AbstractC0125h.java L/d.java L/h.java L/i.java M4/h.java M4/o.java O4/h.java P3/f.java S4/a.java T6/e.java T6/i.java com/bumptech/glide/d.java g2/q.java g3/C0811p.java g7/w.java k2/C1166c.java k2/C1167d.java l0/g.java o2/C1345b.java w2/p.java y0/C1594a.java y0/e.java y0/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	O4/h.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A1/a.java B1/a.java D3/C0033d1.java D3/C0053k0.java D3/X1.java R0/a.java S1/c.java W0/a.java c6/r.java com/amigoexpress/android/center/FirebaseMessagingService.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingDriverActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RidePassengerActivity.java d3/C0698f.java g2/q.java o1/C1343c.java q1/C1399d.java
00091	Retrieve data from broadcast	collection	D3/C0033d1.java a7/d.java
00089	Connect to a URL and receive input stream from the server	command network	D3/RunnableC0026b0.java E5/k.java com/bumptech/glide/load/data/l.java j5/C1151c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	D3/RunnableC0026b0.java E5/k.java Z2/c.java com/bumptech/glide/load/data/l.java j5/C1151c.java
00202	Make a phone call	control	R0/a.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingDriverActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RidePassengerActivity.java
00203	Put a phone number into an intent	control	R0/a.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingDriverActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RidePassengerActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	R0/a.java W0/a.java com/amigoexpress/android/controller/home/pager/mydepartures/booking/BookingDriverActivity.java com/amigoexpress/android/controller/home/pager/mydepartures/ride/RidePassengerActivity.java d3/C0698f.java g2/q.java
00036	Get resource file from res/raw directory	reflection	d3/C0698f.java g2/q.java m3/AbstractC1228a.java t2/C1478b.java
00121	Create a directory	file command	C2/w.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	a7/c.java a7/n.java
00163	Create new Socket and connecting to it	socket	a7/c.java a7/n.java
00012	Read data and put it into a buffer stream	file	l0/g.java
00114	Create a secure socket connection to the proxy address	network command	V6/k.java
00094	Connect to a URL and read data from it	command network	B/c.java D3/RunnableC0026b0.java
00147	Get the time of current location	collection location	h/C0828A.java
00075	Get location of the device	collection location	h/C0828A.java
00115	Get last known location of the device	collection location	h/C0828A.java
00004	Get filename and put it to JSON object	file collection	A2/c.java
00096	Connect to a URL and set request method	command network	E5/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	E5/k.java f3/l.java
00030	Connect to the remote server through the given URL	network	D3/RunnableC0026b0.java com/bumptech/glide/load/data/l.java
00108	Read the input stream from given URL	network command	D3/RunnableC0026b0.java
00025	Monitor the general action to be performed	reflection	a7/d.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://covoiturage-amigoexpress.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1047881112792/namespaces/firebase:fetch?key=AIzaSyAVJ0O8Tdu9aqH4TXwISn1dgl2U4ha5c30 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'ApplePayEnabled': 'true', 'LoginRedesignEnabled': 'true', 'TripListPhotoEnabled': 'false', 'allowEnvironmentSwitch': 'true'}, 'state': 'UPDATE', 'templateVersion': '63'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 192.178.192.101 **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:** 142.250.137.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.livechatinc.com	ok	**IP:** 2.16.170.141 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
api3.amigoexpress.com	ok	**IP:** 204.13.108.99 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.992397 **Longitude:** -96.682106 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 192.178.192.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.139.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.137.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 192.178.192.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 142.250.137.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.137.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 192.178.192.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 142.250.139.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.amigoexpress.com	ok	**IP:** 204.13.108.99 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.992397 **Longitude:** -96.682106 **View:** Google Map
www.google.com	ok	**IP:** 142.250.137.103 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.69.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
covoiturage-amigoexpress.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
play.google.com	ok	**IP:** 142.250.137.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	**IP:** 192.178.192.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.137.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	d3/BinderC0704l.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"api_url" : "https://api3.amigoexpress.com"
"com.google.firebase.crashlytics.mapping_file_id" : "246a50e6421d41f48380fd8780a3fc6c"
"firebase_database_url" : "https://covoiturage-amigoexpress.firebaseio.com"
"google_api_key" : "AIzaSyAVJ0O8Tdu9aqH4TXwISn1dgl2U4ha5c30"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAVJ0O8Tdu9aqH4TXwISn1dgl2U4ha5c30"
"promotions_button_pass" : "Passer"
"settings_key_category_emails" : "key_category_emails"
"settings_key_category_notifications" : "key_category_notifications"
"settings_key_category_phone_verification" : "key_category_phone_verification"
"settings_key_category_privacy" : "key_category_privacy"
"settings_key_category_profile" : "key_category_profile"
"settings_key_category_public_info" : "key_category_public_info"
"settings_key_category_touch_id" : "key_category_touch_id"
"settings_key_list_public_info_name" : "key_public_info_name"
"settings_key_preference_phone_verification" : "key_phone_verification_summary"
"settings_key_preference_privacy_email" : "key_privacy_email_summary"
"settings_key_preference_privacy_phone" : "key_privacy_phone_summary"
"settings_key_preference_profile_public" : "key_profile_public_summary"
"settings_key_preference_public_info_friends" : "key_public_info_friends_summary"

POSSIBLE SECRETS
"settings_key_preference_public_info_name" : "key_public_info_name_summary"
"settings_key_preference_touch_id" : "key_touch_id_summary"
"settings_key_screen_notifications_eval" : "key_notifications_eval"
"settings_key_screen_notifications_ride" : "key_notifications_ride"
"settings_key_screen_notifications_warnings" : "key_notifications_warnings"
"settings_key_screen_privacy_phone" : "key_privacy_phone"
"settings_key_switch_privacy_email_visible" : "key_privacy_email"
"settings_key_switch_profile_public" : "key_profile_public"
"settings_key_switch_public_info_age" : "key_public_info_age"
"settings_key_switch_public_info_city" : "key_public_info_city"
"settings_key_switch_public_info_friends" : "key_public_info_friends"
"settings_key_switch_touch_id" : "key_touch_id"
"settings_notifications_key_category_by_email" : "key_notifications_by_email"
"settings_notifications_key_category_by_notif" : "key_notifications_by_notif"
"settings_notifications_key_category_by_sms" : "key_notifications_by_sms"

POSSIBLE SECRETS
"settings_notifications_key_preference" : "key_notifications_summary"
"settings_notifications_key_preference_by_sms" : "key_notifications_by_sms_summary"
"settings_notifications_key_switch_by_email" : "key_notifications_switch_by_email"
"settings_notifications_key_switch_by_notif" : "key_notifications_switch_by_notif"
aWn6eTaptf03mlbxWA2dTSMPDzxpf6jSPT5UVBVH
470fa2b4ae81cd56ecbcda9735803434cec591fa
AIzaSyDpzZ0kIlLFH0stnQgMNOuSAevZ26liNXY

PLAYSTORE INFORMATION

Title: Kangaride

Score: 4.590909 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Travel & Local **Play Store URL:** com.amigoexpress.android

Developer Details: Covoiturage Amigo Express Inc., Covoiturage+Amigo+Express+Inc., None, https://www.amigoexpress.com/, support@amigoexpress.com,

Release Date: Dec 17, 2019 **Privacy Policy:** Privacy link

Description:

Kangaride – Your Trusted Ride-Sharing Companion Discover the easiest way to find and share rides with Kangaride, the go-to ride-sharing app for comfortable and affordable travel. Whether you're commuting, planning a road trip, or just need a ride, Kangaride connects you with trusted drivers and passengers across Canada. Why Choose Kangaride? • Pay As You Go: With Kangaride's flexible token system, you only pay when you book a ride. Purchase tokens that never expire and use them whenever you need a ride—giving you full control over your travel expenses. • Simple Booking: Browse available rides, choose your preferred route, and book your seat in just a few taps. • Safe and Reliable: Drivers are verified to ensure a safe and comfortable journey. See driver reviews before you book. • Flexible Options: Find rides that suit your schedule, or post your own ride offer to share your car with others. • Affordable Travel: Save on travel costs by sharing rides with others heading the same way. • Real-Time Updates: Stay informed with notifications on ride status, and communicate directly with our customer service, available every day of the year. •

Environmentally Friendly: Reduce your carbon footprint by carpooling and making efficient use of available seats. Join the Kangaride community today and start sharing rides with confidence.

SCAN LOGS

Timestamp	Event	Error
2025-11-28 01:11:22	Generating Hashes	OK
2025-11-28 01:11:22	Extracting APK	OK
2025-11-28 01:11:22	Unzipping	OK
2025-11-28 01:11:22	Parsing APK with androguard	OK
2025-11-28 01:11:23	Extracting APK features using aapt/aapt2	OK
2025-11-28 01:11:23	Getting Hardcoded Certificates/Keystores	OK
2025-11-28 01:11:24	Parsing AndroidManifest.xml	OK
2025-11-28 01:11:24	Extracting Manifest Data	OK

2025-11-28 01:11:24	Manifest Analysis Started	OK
2025-11-28 01:11:24	Reading Network Security config from network_security_config.xml	OK
2025-11-28 01:11:24	Parsing Network Security config	OK
2025-11-28 01:11:24	Performing Static Analysis on: AmigoExpress (com.amigoexpress.android)	OK
2025-11-28 01:11:26	Fetching Details from Play Store: com.amigoexpress.android	OK
2025-11-28 01:11:26	Checking for Malware Permissions	OK
2025-11-28 01:11:26	Fetching icon path	OK
2025-11-28 01:11:26	Library Binary Analysis Started	OK
2025-11-28 01:11:26	Reading Code Signing Certificate	OK
2025-11-28 01:11:27	Running APKiD 3.0.0	OK
2025-11-28 01:11:29	Detecting Trackers	OK

2025-11-28 01:11:29	Decompiling APK to Java with JADX	OK
2025-11-28 01:11:47	Converting DEX to Smali	OK
2025-11-28 01:11:47	Code Analysis Started on - java_source	OK
2025-11-28 01:11:48	Android SBOM Analysis Completed	OK
2025-11-28 01:11:52	Android SAST Completed	OK
2025-11-28 01:11:52	Android API Analysis Started	OK
2025-11-28 01:11:53	Android API Analysis Completed	OK
2025-11-28 01:11:54	Android Permission Mapping Started	OK
2025-11-28 01:11:55	Android Permission Mapping Completed	OK
2025-11-28 01:11:55	Android Behaviour Analysis Started	OK
2025-11-28 01:11:57	Android Behaviour Analysis Completed	OK

2025-11-28 01:11:57	Extracting Emails and URLs from Source Code	OK
2025-11-28 01:11:59	Email and URL Extraction Completed	OK
2025-11-28 01:11:59	Extracting String data from APK	OK
2025-11-28 01:11:59	Extracting String data from Code	OK
2025-11-28 01:11:59	Extracting String values and entropies from Code	OK
2025-11-28 01:12:01	Performing Malware check on extracted domains	OK
2025-11-28 01:12:03	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.