ANDROID STATIC ANALYSIS REPORT

Farmacias del Ahorro (9.7.0)

File Name:	mx.com.fahorro2_5030331.apk
Package Name:	mx.com.fahorro2
Scan Date:	Sept. 1, 2025, 2:44 p.m.
App Security Score:	47/100 (MEDIUM RISK)

Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	20	4	2	1

FILE INFORMATION

File Name: mx.com.fahorro2_5030331.apk
Size: 35.5MB
MD5: f85fc539c5ff744067980a3fcbbd0955
SHA1: 664dc1e639721c66b486082931d88b9cf9539b46
SHA256: a544834adf69253e37010dd45532515ad5e411b18b0975288006dc6135ecbe79

APP INFORMATION

App Name: Farmacias del Ahorro
Package Name: mx.com.fahorro2

Main Activity: com.app.farmaciasdelahorro.farmacias_del_ahorro.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 9.7.0
Android Version Code: 5030331

APP COMPONENTS

Activities: 18
Services: 17
Receivers: 12
Providers: 8
Exported Activities: 4
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=MX, ST=DF, L=Mexico, O=iNetCorp, OU=Desarrollo, CN=Victor Garcia
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-06-12 10:20:31+00:00
Valid To: 2039-06-06 10:20:31+00:00
Issuer: C=MX, ST=DF, L=Mexico, O=iNetCorp, OU=Desarrollo, CN=Victor Garcia
Serial Number: 0x24e00e1f
Hash Algorithm: sha256
md5: 25f30fd1a2291674663a7072143fd5b8
sha1: 7d2b4eb1d169f7e56efb9e4da42ca1a59d617548
sha256: d114a3a366db8a8b6859c4037d744d68a41a3fd775cb9e57d9fe3d0dfbe9e7d4
sha512: 2f894935beb01bf026632a64ca7b6e4ccd425c9ed3e89ea80ae7f61bfa3b637beadd50a05eb7f208021e27f64a3facce49e244646b1496cbcd9ba9237a8a2c65
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8eacbaec60cf51eec6c853be1f10ddf0c734880023b65935ed2e9e3a34c69d8d
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.VIDEO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.AUDIO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
mx.com.fahorro2.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>f85fc539c5ff744067980a3fcbbd0955.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
<tr><td>Obfuscator</td><td>DexGuard</td></tr>
</table>
</td></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.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.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.BOARD check
possible Build.SERIAL check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.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>Obfuscator</td><td>DexGuard</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.app.farmaciasdelahorro.farmacias_del_ahorro.MainActivity	Schemes: https://, Hosts: @string/host, Path Patterns: .*\\.html,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.mx.com.fahorro2,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	aeafa3b24e094478f9b967c632c79a50-1987663961.us-east-2.elb.amazonaws.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	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	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.
4	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 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	Activity (com.example.miniapp_example.MainActivity) 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.
6	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.
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
8	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
9	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.
10	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: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/r0.java a9/a.java ac/b.java ac/c.java ac/i.java ac/r.java ac/t.java ac/v.java ac/y.java ac/z.java ad/h.java af/a1.java af/b1.java af/d0.java af/e.java af/g0.java af/i0.java af/j1.java af/k0.java af/m1.java af/q0.java af/u0.java af/v1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ai/x0.java aj/a.java b1/b.java b4/c.java bc/c0.java bc/f.java bc/h0.java bc/k.java bc/l.java bc/m0.java bc/p.java bc/y.java bf/f.java bf/n.java c4/d.java c4/f.java c4/g.java c7/m.java c8/a.java cg/b.java com/adobe/marketing/mobile/assurance/internal/d.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/b.java com/baseflow/geolocator/j.java com/baseflow/geolocator/m.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java com/it_nomads/fluttersecurestorage/ciphers/h.java com/lyokone/location/FlutterLocationService.java com/lyokone/location/a.java com/lyokone/location/b.java com/lyokone/location/c.java com/lyokone/location/d.java com/newrelic/agent/android/harvest/l.java com/newrelic/agent/android/harvest/u.java com/newrelic/agent/android/logging/b.java com/newrelic/agent/android/logging/e.java com/newrelic/agent/android/logging/p.java com/pichillilorenzo/flutter_inappwebview_android/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/content_blocker/ContentBlockerHandler.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java com/pichillilorenzo/flutter_inappwebview_android/service_worker/ServiceWorkerManager.java com/pichillilorenzo/flutter_inappwebview_android/types/WebViewAssetLoaderExt.java com/pichillilorenzo/flutter_inappwebview_android/webview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClientCompat.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.java d/a.java d3/f.java d7/b.java dg/c.java dk/a.java dn/a.java e4/a.java ec/a.java ef/g.java ek/b0.java ek/d0.java ek/i.java en/d.java en/q.java f7/a.java f7/q.java f7/s.java f7/v.java f9/k.java g2/m0.java g8/e0.java g8/n0.java g8/o0.java g8/v.java gi/a.java gi/e.java h7/e.java h7/u.java hf/s.java i0/a0.java i4/c.java i9/a.java ic/b.java ii/a.java ii/b.java ij/b.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/b.java io/flutter/plugins/firebase/messaging/i.java io/flutter/plugins/googlemaps/GoogleMapController.java io/flutter/plugins/googlemaps/e0.java io/flutter/plugins/googlesignin/e.java io/flutter/plugins/imagepicker/o.java io/flutter/plugins/pathprovider/i.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/o3.java j3/d.java j4/a.java jc/g.java jc/r.java jc/s.java jn/g.java k0/d.java k4/a.java k4/k.java k8/c.java ke/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ke/b.java ke/c.java ki/d.java l/c.java l3/x.java lg/a.java lg/e.java li/e.java li/q.java lj/a.java lj/g.java ll/a.java mc/f.java n1/g.java n1/w.java n5/e.java n5/k.java nb/r.java nc/d.java nl/i.java o3/e.java o4/n.java o5/b.java o5/g.java o7/a.java og/d0.java og/g.java og/g0.java og/i0.java og/k.java og/y.java p5/e.java p8/c.java pd/d.java pg/a.java q7/c1.java q7/g.java q7/i0.java q7/n0.java q7/s0.java q8/e0.java q8/f0.java q8/y.java qb/a.java qb/d.java qd/b.java qg/c.java qg/f.java qi/c.java qi/o.java qk/a.java qk/e.java r6/b.java r7/d.java r7/g.java r7/n.java r7/o0.java r7/s.java rb/o.java rc/e.java s2/f0.java s3/c.java sc/i0.java sd/g.java sk/b.java t4/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tc/e.java te/g.java u6/a.java u7/l.java u8/b.java v4/q.java v6/g.java v7/e.java v7/f.java v8/a.java vi/b.java vi/e.java w4/a.java w6/a.java w6/b.java x7/a.java xc/a.java y/o0.java y6/e.java y6/f.java yb/f.java yc/a.java z5/a.java z7/f.java z7/i.java z7/j.java z7/m.java zi/k.java
2	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	b1/i1.java b1/j2.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/newrelic/agent/android/harvest/n.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview_android/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/HttpAuthResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/URLCredential.java jf/e.java jf/w.java ng/b.java p003if/b.java q5/a.java r2/h.java r2/q0.java t7/g.java x5/f.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	d8/b.java q7/b.java q7/c1.java q7/j.java q7/p0.java q7/t0.java q8/e0.java x7/j.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	app/tango/o/clearWallpaper.java app/tango/o/sendBroadcast.java en/r.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	cg/b.java kk/e.java p8/a.java
6	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	app/tango/o/getPackageManager.java bk/d.java com/distil/protection/android/Protection.java g6/a.java g8/n0.java jm/a.java jm/b.java km/a.java mj/q.java q7/r.java r9/q1.java sa/r0.java va/b.java
7	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	com/adobe/marketing/mobile/internal/util/k.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java ek/i.java m9/m0.java m9/t0.java t5/d.java zi/i.java
8	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/it_nomads/fluttersecurestorage/ciphers/h.java xa/a.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	bn/i.java ck/b.java hf/i.java
10	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	r7/e.java z7/m.java
11	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	bn/i.java bn/l.java cn/a.java g8/n0.java io/flutter/plugins/pathprovider/a.java io/flutter/plugins/pathprovider/i.java li/e.java
12	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	io/flutter/plugin/editing/h.java io/flutter/plugin/platform/m.java
13	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	a0/t.java cg/c.java
14	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bn/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	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/adobe/marketing/mobile/assurance/internal/g0.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	ck/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	af/f1.java bc/g.java com/adobe/marketing/mobile/assurance/internal/AssuranceExtension.java com/adobe/marketing/mobile/messaging/MessagingPushTrackerActivity.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java e7/a.java f7/a.java f7/q.java f7/v.java g8/a.java g8/e0.java g8/n0.java g8/o0.java g8/s0.java io/flutter/plugins/imagepicker/l.java k4/a.java m6/b.java m7/a.java nl/h.java q8/c.java qk/e.java z4/a.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java q7/i0.java u7/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	app/tango/o/EncryptStrings.java com/adobe/marketing/mobile/assurance/internal/b.java com/newrelic/agent/android/harvest/o.java com/pichillilorenzo/flutter_inappwebview_android/Util.java dg/c.java mb/s.java oi/c.java q7/i0.java t7/g.java
00091	Retrieve data from broadcast	collection	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java g8/e0.java q8/k0.java qk/e.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bc/g.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java e7/a.java f7/a.java f7/q.java f7/v.java g8/n0.java g8/o0.java k4/a.java m6/b.java m7/a.java nl/h.java z4/a.java
00013	Read file and put it into a stream	file	a0/t.java a8/j.java app/tango/o/deleteDatabase.java app/tango/o/getCodeCacheDir.java app/tango/o/n.java app/tango/o/valueOf.java b6/b.java cg/c.java cm/l.java cm/n.java cn/a.java com/adobe/marketing/mobile/internal/util/f.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d8/a.java hf/b0.java i8/k.java mb/g.java mb/h0.java mf/e.java mj/o.java of/a.java p003if/f.java r7/g.java u3/m.java u8/b.java w5/d.java z7/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00023	Start another application from current application	reflection control	m7/a.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/assurance/internal/d.java g8/n0.java mj/c.java z5/i.java
00022	Open a file from given absolute path of the file	file	a0/t.java app/tango/o/getCodeCacheDir.java bn/h.java bn/l.java com/adobe/marketing/mobile/internal/util/f.java com/newrelic/agent/android/logging/e.java com/newrelic/agent/android/logging/p.java io/flutter/plugins/pathprovider/i.java mj/i.java p003if/f.java u3/m.java u8/a.java u8/b.java z8/a.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/m.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/m.java
00089	Connect to a URL and receive input stream from the server	command network	app/tango/o/EncryptStrings.java com/adobe/marketing/mobile/assurance/internal/b.java com/newrelic/agent/android/harvest/o.java dg/c.java mb/s.java p8/c.java t7/g.java
00109	Connect to a URL and get the response code	network command	app/tango/o/EncryptStrings.java com/adobe/marketing/mobile/assurance/internal/b.java com/newrelic/agent/android/harvest/o.java dg/c.java mb/s.java oi/c.java qb/d.java t7/g.java vi/c.java yb/e.java
00147	Get the time of current location	collection location	com/lyokone/location/a.java
00012	Read data and put it into a buffer stream	file	app/tango/o/getCodeCacheDir.java r7/g.java z7/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	bc/g.java bn/i.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java e7/a.java f7/a.java f7/q.java g8/a.java g8/n0.java g8/o0.java g8/s0.java mb/h0.java
00102	Set the phone speaker on	command	ak/e0.java
00056	Modify voice volume	control	ak/e0.java
00108	Read the input stream from given URL	network command	com/newrelic/agent/android/harvest/o.java hj/f.java mb/s.java
00004	Get filename and put it to JSON object	file collection	a8/f.java bn/i.java bn/l.java i8/c.java m8/a.java
00125	Check if the given file path exist	file	a8/f.java
00014	Read file into a stream and put it into a JSON object	file	a8/j.java cg/c.java d8/a.java i8/k.java of/a.java p003if/f.java
00028	Read file from assets directory	file	mb/c.java
00030	Connect to the remote server through the given URL	network	com/pichillilorenzo/flutter_inappwebview_android/Util.java mb/s.java
00094	Connect to a URL and read data from it	command network	com/newrelic/agent/android/harvest/o.java com/pichillilorenzo/flutter_inappwebview_android/Util.java lf/a.java mb/s.java
00015	Put buffer stream (data) to JSON object	file	g8/n0.java
00009	Put data in cursor to JSON object	file	bn/i.java g8/n0.java
00191	Get messages in the SMS inbox	sms	g8/a.java g8/e0.java g8/n0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	nb/r0.java
00005	Get absolute path of file and put it to JSON object	file	bn/h.java bn/l.java p003if/f.java
00189	Get the content of a SMS message	sms	g8/e0.java
00188	Get the address of a SMS message	sms	g8/e0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	g8/e0.java
00200	Query data from the contact list	collection contact	g8/e0.java
00187	Query a URI and check the result	collection sms calllog calendar	g8/e0.java
00201	Query data from the call log	collection calllog	g8/e0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	g8/e0.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/f.java l3/x.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java l3/x.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	bn/i.java
00130	Get the current WIFI information	wifi collection	bn/i.java bn/l.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	bn/i.java
00076	Get the current WiFi information and put it into JSON	collection wifi	bn/i.java bn/l.java
00082	Get the current WiFi MAC address	collection wifi	bn/i.java
00131	Get location of the current GSM and put it into JSON	collection location	bn/l.java
00042	Query WiFi BSSID and scan results	collection wifi	bn/l.java
00137	Get last known location of the device	location collection	bn/l.java
00033	Query the IMEI number	collection	bn/l.java
00139	Get the current WiFi id	collection wifi	bn/l.java
00115	Get last known location of the device	collection location	bn/l.java
00066	Query the ICCID number	collection	bn/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00135	Get the current WiFi id and put it into JSON.	wifi collection	bn/l.java
00067	Query the IMSI number	collection	bn/l.java
00099	Get location of the current GSM and put it into JSON	collection location	bn/l.java
00083	Query the IMEI number	collection telephony	bn/l.java
00113	Get location and put it into JSON	collection location	bn/l.java
00016	Get location info of the device and put it to JSON object	location collection	bn/l.java
00202	Make a phone call	control	f7/v.java
00203	Put a phone number into an intent	control	f7/v.java
00162	Create InetSocketAddress object and connecting to it	socket	mj/k.java
00163	Create new Socket and connecting to it	socket	mj/k.java z5/q.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00153	Send binary data over HTTP	http	com/adobe/marketing/mobile/assurance/internal/b.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://farmacias-del-ahorro-a50ee.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/735787215025/namespaces/firebase:fetch?key=AIzaSyDL892i_Qh2AO4_c-2TW3QUFWenn_rIX5s is enabled. Ensure that the configurations are not sensiti 'MIN_POSTCODE_LOCATION_DISTANCE': '2', 'NIMBO_BEAUTY_AND_SKIN_URL': 'https://app.nimbo-x.com/o/fahorro-derma', 'NIMBO_DENTAL_HEALTH_URL': 'https://app.nimbo-x.com/o/fahorro-odonto', 'NIMBO_MENTAL_HEALTH_URL': 'https:// in/flyer_images/531211937293991669_image_1500x692.webp","promotionNameEng":"Derma","promotionNameSpn":"Derma","timerMsgEs":" Esta oferta termina en","timerMsgEn":"This offer ends in","eventName":"Drama","startDate":"May 2 'https://api-m.sandbox.paypal.com', 'base_recurrent_adyen_payment_url': 'https://a6bbe4b3c33067e0-FarmaciasDelAhorro-pal-live.adyenpayments.com/pal/servlet/Recurring/v68', 'base_rest_url': 'https://fdainventarioprod.omni.pro/Omnipro/ mda","frequent_questions":"https://www.fahorro.com/preguntas-frecuentes","about":"https://www.fahorro.com/quienessomos","antigen_terms_consent":"https://www.fahorro.com/media/folleto/Aviso_Consentimiento_ESP.pdf","ahorrolab_re "dial_code": "+973", "code": "BH" }, { "name": "Bangladesh", "dial_code": "+880", "code": "BD" }, { "name": "Barbados", "dial_code": "+1 246", "code": "BB" }, { "name": "Belarus", "dial_code": "+375", "code": "BY" }, { "name": "Belgium", "dial_code": " "dial_code": "+20", "code": "EG" }, { "name": "El Salvador", "dial_code": "+503", "code": "SV" }, { "name": "Equatorial Guinea", "dial_code": "+240", "code": "GQ" }, { "name": "Eritrea", "dial_code": "+291", "code": "ER" }, { "name": "Estonia", "dial_code' "name": "Kiribati", "dial_code": "+686", "code": "KI" }, { "name": "Kuwait", "dial_code": "+965", "code": "KW" }, { "name": "Kyrgyzstan", "dial_code": "+996", "code": "KG" }, { "name": "Latvia", "dial_code": "+371", "code": "LV" }, { "name": "Lebanon", "d "dial_code": "+1 670", "code": "MP" }, { "name": "Norway", "dial_code": "+47", "code": "NO" }, { "name": "Oman", "dial_code": "+968", "code": "OM" }, { "name": "Pakistan", "dial_code": "+92", "code": "PK" }, { "name": "Palau", "dial_code": "+680", "co "name": "Trinidad and Tobago", "dial_code": "+1 868", "code": "TT" }, { "name": "Tunisia", "dial_code": "+216", "code": "TN" }, { "name": "Turkey", "dial_code": "+90", "code": "TR" }, { "name": "Turkmenistan", "dial_code": "+993", "code": "TM" }, { "na Yugoslav Republic of", "dial_code": "+389", "code": "MK" }, { "name": "Micronesia, Federated States of", "dial_code": "+691", "code": "FM" }, { "name": "Moldova, Republic of", "dial_code": "+373", "code": "MD" }, { "name": "Mozambique", "dial_code '["gap182@gmail.com","Ariel.torres.omni@gmail.com","vargas.felipe@omni.pro","vega.julian@omni.pro","gustavo.parra@omni.pro","eddier.caicedo@omni.pro","diego.llanten@omni.pro","felipe.rincon@omni.pro","salazarisidro505@gmail.com production.s3.amazonaws.com/icons/wallet.svg","code":"COLLECTPOINTS","title":"Acumule y gane","description":"Acumule 100 pesos en su registro promocional y le daremos 100 pesos de saldo."},{"image":"https://fda-panel-production.s3.am '{"minScaleFactor":0.3,"maxScaleFactor":1.7,"navbar":1.2,"header":1.5,"headerCart":1,"homeCategories":1,"homeSliders":1.5,"productCard":1,"onboardRoute":1.5,"loginRoute":1.7,"forgotPasswordRoute":1.5,"selectCountryCodeRoute":1.5,"signU 'search_history_limit': '40', 'show_branch_services': 'false', 'show_category_in_search_history': 'true', 'show_content_recurring_order': 'false', 'show_delivery_time_schedule': 'false', 'show_estimated_delivery_time': 'false', 'show_global_orders': 'fals 'https://fda-fastapi.s3.amazonaws.com/banners/splash+programado+v2+941x1600-01+(1)+(1).png', 'use_auth_products': 'false', 'use_bool_for_lab_filter': 'true', 'use_get_filtered_by_is_laboratory': 'true', 'version_feature_notification': 'V2', 'visible_

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

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
graph-video.s	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
blobs.griffon.adobe.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
graph.s	ok	No Geolocation information available.
device.griffon.adobe.com	ok	**IP:** 13.224.53.87 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
default.url	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
c.sandbox.paypal.com	ok	**IP:** 151.101.3.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
farmacias-del-ahorro-a50ee.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
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
c.paypal.com	ok	**IP:** 151.101.129.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.58 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.141.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.paypalobjects.com	ok	**IP:** 172.64.153.163 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.fahorro.com	ok	**IP:** 45.223.161.233 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.143 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
b.stats.paypal.com	ok	**IP:** 34.106.92.18 **Country:** United States of America **Region:** Utah **City:** Salt Lake City **Latitude:** 40.760780 **Longitude:** -111.891052 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.207.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.38.161.73 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
aomedia.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
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	bc/x.java

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130

HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "94e919bc4cc1dfe23d898049ff19aa86"
"firebase_database_url" : "https://farmacias-del-ahorro-a50ee.firebaseio.com"
"gmaps_api_key" : "AIzaSyAAi7dTFyiiKr949taYvjRZSftCdlNKkJs"
"google_api_key" : "AIzaSyDL892i_Qh2AO4_c-2TW3QUFWenn_rIX5s"
"google_crash_reporting_api_key" : "AIzaSyDL892i_Qh2AO4_c-2TW3QUFWenn_rIX5s"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
389C9738-A761-44DE-8A66-1668CFD67DA1
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
470fa2b4ae81cd56ecbcda9735803434cec591fa
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c56fb7d591ba6704df047fd98f535372fea00211

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
36864200e0eaf5284d884a0e77d31646
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
cc2751449a350f668590264ed76692694a80308a
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403803403728088927070054490
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
016d026c-c477-4a7e-9ced-c8000f126e62

PLAYSTORE INFORMATION

Title: Farmacias del Ahorro

Score: 3.65 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** mx.com.fahorro2

Developer Details: Farmacias del Ahorro, Farmacias+del+Ahorro, None, https://www.fahorro.com, appmovil@fahorro.com.mx,

Release Date: Jul 15, 2020 **Privacy Policy:** Privacy link

Description:

With the Farmacias del Ahorro App, you will have well-being, health, prevention and beauty at your fingertips. Browse through the different product categories and find what you are looking for. Scan products and add them to your shopping cart easily. FREE SHIPPING IN ALL MEXICO Home delivery is FREE and we do not raise prices for it. Send wellness to who you love the most in less than 90 minutes. Make your order from your cell phone and check the status at all times, from the moment it is processed until it reaches your door. PAYMENT METHODS Make your purchase safely using credit / debit card or on delivery using cash. SCHEDULED SHIPMENTS Schedule your recurring orders from the App and receive them at your door whenever you want. LOYALTY PROGRAM Always carry our Loyalty Program Card with you, use it in all your purchases online or at a branch and accumulate virtual money. Virtual Loyalty Program Card features: check your balance, 100 +100 balance, account statement and free gifts with our loyalty plan. FREE MEDICAL GUIDANCE SERVICE Because we want you well protected, we have implemented a free Remote Orientation Service. Schedule an orientation with an available doctor to treat you without having to leave home. BRANCH SEARCH Find the branch closest to your location. Check hours of attention and medical guidance service.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:44:51	Generating Hashes	OK
2025-09-01 14:44:51	Extracting APK	OK
2025-09-01 14:44:51	Unzipping	OK
2025-09-01 14:44:52	Parsing APK with androguard	OK
2025-09-01 14:44:52	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:44:52	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 14:44:54	Parsing AndroidManifest.xml	OK

2025-09-01 14:44:54	Extracting Manifest Data	OK
2025-09-01 14:44:54	Manifest Analysis Started	OK
2025-09-01 14:44:54	Reading Network Security config from network_security_config.xml	OK
2025-09-01 14:44:54	Parsing Network Security config	OK
2025-09-01 14:44:54	Performing Static Analysis on: Farmacias del Ahorro (mx.com.fahorro2)	OK
2025-09-01 14:44:55	Fetching Details from Play Store: mx.com.fahorro2	OK
2025-09-01 14:44:57	Checking for Malware Permissions	OK
2025-09-01 14:44:57	Fetching icon path	OK
2025-09-01 14:44:57	Library Binary Analysis Started	OK
2025-09-01 14:44:57	Reading Code Signing Certificate	OK
2025-09-01 14:44:57	Running APKiD 2.1.5	OK
2025-09-01 14:45:02	Detecting Trackers	OK
2025-09-01 14:45:05	Decompiling APK to Java with JADX	OK
2025-09-01 14:45:56	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 14:45:56	Decompiling classes2.dex with JADX	OK
2025-09-01 14:46:00	Decompiling classes4.dex with JADX	OK
2025-09-01 14:46:02	Decompiling classes.dex with JADX	OK

2025-09-01 14:46:11	Decompiling classes3.dex with JADX	OK
2025-09-01 14:46:21	Decompiling classes2.dex with JADX	OK
2025-09-01 14:46:25	Decompiling classes4.dex with JADX	OK
2025-09-01 14:46:26	Decompiling classes.dex with JADX	OK
2025-09-01 14:46:35	Decompiling classes3.dex with JADX	OK
2025-09-01 14:46:45	Converting DEX to Smali	OK
2025-09-01 14:46:45	Code Analysis Started on - java_source	OK
2025-09-01 14:46:48	Android SBOM Analysis Completed	OK
2025-09-01 14:46:56	Android SAST Completed	OK
2025-09-01 14:46:56	Android API Analysis Started	OK
2025-09-01 14:47:03	Android API Analysis Completed	OK
2025-09-01 14:47:04	Android Permission Mapping Started	OK
2025-09-01 14:47:13	Android Permission Mapping Completed	OK
2025-09-01 14:47:13	Android Behaviour Analysis Started	OK
2025-09-01 14:47:23	Android Behaviour Analysis Completed	OK
2025-09-01 14:47:23	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:47:26	Email and URL Extraction Completed	OK

2025-09-01 14:47:26	Extracting String data from APK	OK
2025-09-01 14:47:26	Extracting String data from Code	OK
2025-09-01 14:47:26	Extracting String values and entropies from Code	OK
2025-09-01 14:47:29	Performing Malware check on extracted domains	OK
2025-09-01 14:47:32	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.