ANDROID STATIC ANALYSIS REPORT

app_icon

Express Scripts (12.20.0)

File Name:	com.medco.medcopharmacy_883.apk
Package Name:	com.medco.medcopharmacy
Scan Date:	Aug. 31, 2025, 3:16 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	18	2	4	1

FILE INFORMATION

File Name: com.medco.medcopharmacy_883.apk
Size: 23.62MB
MD5: 2f8dc9099d3cd093c39db06497411b6b
SHA1: 16fd2fbe0d3a22d26e627b7f7e4c3ac3ce8c0b04
SHA256: ed7d7b9b31f275ed07f5cff487aa21b36f98576410f5de7ce9e86540fde133a8

APP INFORMATION

App Name: Express Scripts
Package Name: com.medco.medcopharmacy
Main Activity: com.express_scripts.patient.ui.launch.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 12.20.0

Android Version Code: 883

APP COMPONENTS

Activities: 6
Services: 11
Receivers: 15
Providers: 4
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=New Jersey, L=Franklin Lakes, O=Medco Health Solutions, Inc., OU=Mobile Development, CN=Medco Mobile Apps
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-01-26 16:36:54+00:00
Valid To: 2038-06-13 16:36:54+00:00
Issuer: C=US, ST=New Jersey, L=Franklin Lakes, O=Medco Health Solutions, Inc., OU=Mobile Development, CN=Medco Mobile Apps
Serial Number: 0x4d404da6
Hash Algorithm: sha1
md5: 143f76e642c721f95433996ea2151c5a
sha1: f0482d4b784594bddbb7a1b191773a6ae17c9af8
sha256: 436fd28bf710a297b2fc61c84485409ba7ed6424b1e326659514af2b7a4240be
sha512: 828c2761f2b04e6cc101ecaa36e317d882345517799aabbb27600a664a434efa9ba606caa277db604cbc0a37f0433c724882fe824c3cebdafa4c41ca794ced2e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f963da8fd8e58c7d2285da492c2a79a4e3930d1c3129a6b16cc90706f9d42fe9
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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_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

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.medco.medcopharmacy.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>2f8dc9099d3cd093c39db06497411b6b.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>emulator file check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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 Build.TAGS check network operator name check emulator file check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.express_scripts.patient.ui.launch.SplashActivity	Schemes: esrx://, https://, com.medco.medcopharmacy.braintree://, Hosts: esrx.app.link,
com.braintreepayments.api.BraintreeDeepLinkActivity	Schemes: com.medco.medcopharmacy.braintree.deeplinkhandler://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	express-scripts.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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.
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	App Link assetlinks.json file not found [android:name=com.express_scripts.patient.ui.launch.SplashActivity] [android:host=https://esrx.app.link]	high	App Link asset verification URL (https://esrx.app.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
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	Activity (com.braintreepayments.api.BraintreeDeepLinkActivity) 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	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Activity (androidx.compose.ui.tooling.PreviewActivity) 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	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: 9 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	b8/k.java g6/c.java g9/c.java g9/e.java z7/d.java zh/m0.java zh/t0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/p.java com/express_scripts/core/data/local/account/CreateAccountV2Response.java com/express_scripts/core/data/local/auth/AuthResponse.java com/express_scripts/core/data/local/cache/FragmentScopedCacheManagerKeys.java com/express_scripts/core/data/remote/account/PaytientSsoTokenResponse.java com/express_scripts/core/data/remote/registration/CreateAccountRequest.java com/express_scripts/core/data/remote/registration/DeleteAccountRequest.java com/express_scripts/core/data/remote/registration/UpdateAccountRequest.java com/express_scripts/patient/ui/digitalidcard/main/a.java com/launchdarkly/sdk/LDContext.java com/okta/authfoundation/client/DeviceTokenProvider.java com/okta/authfoundation/credential/SharedPreferencesTokenStorage.java com/okta/idx/sdk/api/model/I18NMessage.java d3/g.java d3/p0.java e1/b3.java e1/u1.java e8/f.java qa/b.java qa/d.java v0/u0.java v8/t3.java w7/a.java zp/f1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aj/d.java b4/c.java b4/i.java b4/t.java b6/a.java c4/a.java com/launchdarkly/sdk/android/n0.java d4/c.java d4/d.java d4/h.java dj/g.java dk/f.java dk/n.java e1/b.java e3/m0.java e4/d.java e4/f.java e4/g.java e4/k.java e5/a.java e6/b.java f/e.java f3/a.java f6/h.java g5/c.java g6/d.java gi/f.java h6/a.java h8/a.java hq/a.java i/f.java i/h.java i/r.java i/w.java iq/b.java k3/c.java k5/a.java k6/b.java l4/n.java l6/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	l6/m0.java m4/b.java n/g.java n9/e.java o/c.java p/C0950y.java p/U.java p/c0.java p/g1.java p/q0.java p/s0.java p/t0.java p/v.java p/w0.java p/y.java p2/n0.java p4/f1.java p4/x.java p4/x0.java p4/z1.java pk/b.java pl/e0.java pq/p.java pr/a.java q4/n.java qk/b.java r0/t1.java r1/f.java r3/d.java r5/a.java rk/c.java sh/k.java t/d.java t/e.java t/f.java t/h.java t/i.java t/k.java t/l.java t6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tj/a.java tj/b.java tj/c.java u3/f.java u4/c.java u6/j.java u8/a.java uk/a0.java uk/b1.java uk/c.java uk/c0.java uk/d.java uk/e0.java uk/e1.java uk/g.java uk/j0.java uk/l.java uk/n.java uk/p0.java uk/r0.java uk/s0.java uk/t0.java uk/w0.java uk/x0.java v4/j.java v5/n.java v8/r0.java v8/w1.java vh/a.java vl/g.java vl/i.java x3/a.java y4/d.java yi/a.java yj/e.java z5/q.java z5/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	com/apiguard3/internal/ce.java com/apiguard3/internal/setImportantForAutofill.java com/express_scripts/patient/notification/a.java com/okta/commons/http/MimeTypeUtils.java f9/a.java f9/b.java m8/a.java tm/a.java tm/b.java um/a.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	a9/b.java el/o.java jq/i.java v8/i3.java
6	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/d.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/apiguard3/internal/setAccessibilityDelegate.java fq/a0.java fq/k0.java
8	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	q2/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	qk/b.java uk/a0.java yb/n.java
10	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	qk/c.java z5/u.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	fq/a0.java y8/y.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fq/a0.java
13	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	fg/e.java t/i.java
14	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	fq/u.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	jh/g0.java lh/z.java
00161	Perform accessibility service action on accessibility node info	accessibility service	q4/n.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	q4/n.java
00078	Get the network operator name	collection telephony	h8/i.java j7/b.java m9/a.java vl/f0.java
00091	Retrieve data from broadcast	collection	com/express_scripts/patient/ui/a.java fc/a.java vl/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b4/c.java b6/b.java b8/f.java com/apiguard3/internal/setAccessibilityDelegate.java d8/d.java e4/k.java e5/a.java j8/b.java mm/m.java okio/Okio__JvmOkioKt.java qk/c.java z5/u.java
00012	Read data and put it into a buffer stream	file	com/apiguard3/internal/setAccessibilityDelegate.java e5/a.java
00094	Connect to a URL and read data from it	command network	com/apiguard3/internal/setAccessibilityDelegate.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adobe/marketing/mobile/assurance/internal/AssuranceExtension.java fc/c.java oe/a.java p8/b.java q2/j0.java uk/c.java v8/p0.java vl/c.java yl/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	fc/c.java p8/b.java uk/c.java v8/p0.java vl/c.java
00036	Get resource file from res/raw directory	reflection	fc/c.java fq/a0.java uk/c.java vl/c.java
00003	Put the compressed bitmap data into JSON object	camera	wl/b.java
00163	Create new Socket and connecting to it	socket	h8/q.java
00022	Open a file from given absolute path of the file	file	b8/f.java com/apiguard3/internal/setAutofillId.java com/launchdarkly/sdk/android/l0.java fq/z.java g6/d.java pl/e0.java rc/h1.java z5/u.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	pl/p.java
00115	Get last known location of the device	collection location	fq/k0.java i/w.java wa/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00147	Get the time of current location	collection location	i/w.java
00075	Get location of the device	collection location	i/w.java
00026	Method reflection	reflection	ln/a.java ln/b.java
00079	Hide the current app's icon	evasion	i/f.java
00005	Get absolute path of file and put it to JSON object	file	fq/z.java
00035	Query the list of the installed packages	reflection	fg/i.java
00191	Get messages in the SMS inbox	sms	sl/c.java
00014	Read file into a stream and put it into a JSON object	file	qk/c.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	fq/a0.java
00130	Get the current WIFI information	wifi collection	fq/a0.java fq/k0.java
00009	Put data in cursor to JSON object	file	fq/a0.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	fq/a0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	fq/a0.java fq/k0.java
00076	Get the current WiFi information and put it into JSON	collection wifi	fq/a0.java fq/k0.java
00082	Get the current WiFi MAC address	collection wifi	fq/a0.java
00042	Query WiFi BSSID and scan results	collection wifi	fq/k0.java
00137	Get last known location of the device	location collection	fq/k0.java
00139	Get the current WiFi id	collection wifi	fq/k0.java
00066	Query the ICCID number	collection	fq/k0.java
00135	Get the current WiFi id and put it into JSON.	wifi collection	fq/k0.java
00067	Query the IMSI number	collection	fq/k0.java
00113	Get location and put it into JSON	collection location	fq/k0.java
00016	Get location info of the device and put it to JSON object	location collection	fq/k0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/491710468137/namespaces/firebase:fetch?key=AIzaSyBhcptZlQb-q441mB3Y73YHJfd7dcoPjW4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

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
api.sandbox.braintreegateway.com	ok	**IP:** 159.242.242.129 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **View:** Google Map
www-uat.express-scripts.com	ok	**IP:** 167.18.110.66 **Country:** United States of America **Region:** Missouri **City:** Saint Louis **Latitude:** 38.707321 **Longitude:** -90.303543 **View:** Google Map
pay.google.com	ok	**IP:** 142.250.110.92 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www-dev.express-scripts.com	ok	**IP:** 13.224.53.114 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.braintreegateway.com	ok	**IP:** 54.70.36.105 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
blobs.griffon.adobe.com	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

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bf08379irm.bf.dynatrace.com	ok	**IP:** 184.73.58.82 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
c.sandbox.paypal.com	ok	**IP:** 151.101.67.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
any.example.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
cert-xiecomm.paymetric.com	ok	**IP:** 74.120.159.133 **Country:** United States of America **Region:** Ohio **City:** Cincinnati **Latitude:** 39.290581 **Longitude:** -84.334686 **View:** Google Map
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
braintreepayments.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

DOMAIN	STATUS	GEOLOCATION
clientsdk.launchdarkly.com	ok	**IP:** 151.101.1.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
prod.login.express-scripts.com	ok	**IP:** 3.210.168.244 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
xiecomm.paymetric.com	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
c.paypal.com	ok	**IP:** 151.101.65.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.paypal.com	ok	**IP:** 104.18.3.198 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.hhs.gov	ok	**IP:** 2.19.158.16 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
mobileqa.express-scripts.com	ok	No Geolocation information available.
mobile.launchdarkly.com	ok	**IP:** 44.209.144.86 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.33 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.express-scripts.com	ok	**IP:** 167.211.52.57 **Country:** United States of America **Region:** New Jersey **City:** Franklin Lakes **Latitude:** 41.009102 **Longitude:** -74.208122 **View:** Google Map
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
api-m.paypal.com	ok	**IP:** 151.101.67.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
express-scripts.calculator.m3p.health	ok	**IP:** 18.238.109.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	ok	**IP:** 18.238.109.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www-qa.express-scripts.com	ok	No Geolocation information available.
clientstream.launchdarkly.com	ok	**IP:** 76.223.31.44 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
express-scripts.calculator.uat.m3p.health	ok	**IP:** 18.238.96.28 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
mobiledev.express-scripts.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
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
schemas.android.com	ok	No Geolocation information available.
mdlnext.mdlive.com	ok	**IP:** 159.60.141.31 **Country:** Netherlands **Region:** Zuid-Holland **City:** The Hague **Latitude:** 52.076672 **Longitude:** 4.298610 **View:** Google Map
myaccess.dmdc.osd.mil	ok	**IP:** 214.16.194.225 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.966381 **Longitude:** -83.012772 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
assets.adobedtm.com	ok	**IP:** 72.247.97.53 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
ocrportal.hhs.gov	ok	**IP:** 156.40.11.174 **Country:** United States of America **Region:** Maryland **City:** Bethesda **Latitude:** 38.999641 **Longitude:** -77.155083 **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

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229

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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBhcptZlQb-q441mB3Y73YHJfd7dcoPjW4"
"google_crash_reporting_api_key" : "AIzaSyBhcptZlQb-q441mB3Y73YHJfd7dcoPjW4"
"order_details_payment_method_type_masterpass" : "Masterpass"
"prior_auth_documents" : "Documents"
"prior_auth_member" : "Member:"
"prior_auth_of" : "of"
"prior_auth_patient_label" : "Patient"
"prior_auth_quantity" : "Quantity:"
"prior_auth_status_approved_title" : "Approved"
"prior_auth_status_cancelled_title" : "Cancelled"
"prior_auth_status_denied_title" : "Denied"

POSSIBLE SECRETS
"prior_auth_status_withdrawn_title" : "Withdrawn"
"prior_auth_step" : "Step:"
56c8ea595c439f4f70d21d9755ea39fc
624d535e-8cff-44a4-8a65-942a44e45eec
cc4e8b009d2e6bf10134122a5aa6fce5
c103703e120ae8cc73c9248622f3cd1e
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F4041 424344454647484 94A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F80818283 8485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3 C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
b-bca32bf7-d13c-44ac-bd0c-14234503f341
49f946663a8deb7054212b8adda248c6
065b039e1e06945e854870d014261016
9fed89d8cda1441351ad045e3dccecbf

PLAYSTORE INFORMATION

Title: Express Scripts

Score: 4.7587743 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.medco.medcopharmacy

Developer Details: Express Scripts, Inc., Express+Scripts,+Inc., None, http://www.express-scripts.com, memberservices@express-scripts.com,

Release Date: Apr 15, 2011 **Privacy Policy:** Privacy link

Description:

Managing your medicine is easier when our app does it for you. The newly designed Express Scripts app lets you easily and quickly find everything you need for your medicine. It's like having a knowledgeable pharmacist in your pocket. Find a preferred pharmacy, refill your prescription and check your order status—anytime, anywhere. Whatever you're looking for, find it faster on the Express Scripts mobile app. You must have an Express Scripts prescription benefit plan through your health insurance or plan sponsor to use this app. This app and/or some if the features described may not be available for all plans or benefit types.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 03:16:22	Generating Hashes	OK
2025-08-31 03:16:22	Extracting APK	OK
2025-08-31 03:16:22	Unzipping	OK
2025-08-31 03:16:23	Parsing APK with androguard	OK
2025-08-31 03:16:23	Extracting APK features using aapt/aapt2	OK

2025-08-31 03:16:23	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 03:16:26	Parsing AndroidManifest.xml	OK
2025-08-31 03:16:26	Extracting Manifest Data	OK
2025-08-31 03:16:26	Manifest Analysis Started	OK
2025-08-31 03:16:26	Reading Network Security config from network_security_config.xml	OK
2025-08-31 03:16:26	Parsing Network Security config	OK
2025-08-31 03:16:26	Performing Static Analysis on: Express Scripts (com.medco.medcopharmacy)	OK
2025-08-31 03:16:26	Fetching Details from Play Store: com.medco.medcopharmacy	OK
2025-08-31 03:16:27	Checking for Malware Permissions	OK
2025-08-31 03:16:27	Fetching icon path	OK

2025-08-31 03:16:27	Library Binary Analysis Started	OK
2025-08-31 03:16:27	Reading Code Signing Certificate	OK
2025-08-31 03:16:27	Running APKiD 2.1.5	OK
2025-08-31 03:16:29	Detecting Trackers	OK
2025-08-31 03:16:31	Decompiling APK to Java with JADX	OK
2025-08-31 03:29:07	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-31 03:29:07	Decompiling classes2.dex with JADX	OK
2025-08-31 03:29:22	Decompiling classes.dex with JADX	OK
2025-08-31 03:29:34	Decompiling classes3.dex with JADX	OK
2025-08-31 03:29:45	Decompiling classes2.dex with JADX	OK
2025-08-31 03:29:57	Decompiling classes.dex with JADX	OK

2025-08-31 03:30:09	Decompiling classes3.dex with JADX	OK
2025-08-31 03:30:20	Converting DEX to Smali	OK
2025-08-31 03:30:20	Code Analysis Started on - java_source	OK
2025-08-31 03:30:27	Android SBOM Analysis Completed	OK
2025-08-31 03:30:40	Android SAST Completed	OK
2025-08-31 03:30:40	Android API Analysis Started	OK
2025-08-31 03:30:53	Android API Analysis Completed	OK
2025-08-31 03:30:53	Android Permission Mapping Started	OK
2025-08-31 03:31:14	Android Permission Mapping Completed	OK
2025-08-31 03:31:25	Android Behaviour Analysis Started	OK
2025-08-31 03:31:48	Android Behaviour Analysis Completed	OK

2025-08-31 03:31:48	Extracting Emails and URLs from Source Code	OK
2025-08-31 03:32:01	Email and URL Extraction Completed	OK
2025-08-31 03:32:01	Extracting String data from APK	OK
2025-08-31 03:32:01	Extracting String data from Code	OK
2025-08-31 03:32:01	Extracting String values and entropies from Code	OK
2025-08-31 03:32:06	Performing Malware check on extracted domains	OK
2025-08-31 03:32:13	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.