MOBSF

ANDROID STATIC ANALYSIS REPORT

RxSaver (4.4.3)

File Name:	com.lowestmed.android_153.apk
Package Name:	com.lowestmed.android
Scan Date:	Aug. 31, 2025, 1:43 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	11	2	1	1

FILE INFORMATION

File Name: com.lowestmed.android_153.apk
Size: 4.97MB
MD5: e1525d367ab2fd6f09e54bccb1d32d07
SHA1: f3ae5225630fc7b2dfed281dc72aa8ff769ee536
SHA256: 7c9bcb2dadaa1b47d8dab0ccf85b9cc5773dfceadaf0b9a40655686713a15d5c

APP INFORMATION

App Name: RxSaver
Package Name: com.lowestmed.android
Main Activity: com.lowestmed.android.MainActivity
Target SDK: 33
Min SDK: 31
Max SDK:
Android Version Name: 4.4.3

Android Version Code: 153

APP COMPONENTS

Activities: 2
Services: 6
Receivers: 3
Providers: 4
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
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=UT, L=Draper, O=LowestMed, OU=IT, CN=Darren D'Orlando
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-01-16 15:50:44+00:00
Valid To: 2037-01-09 15:50:44+00:00
Issuer: C=US, ST=UT, L=Draper, O=LowestMed, OU=IT, CN=Darren D'Orlando
Serial Number: 0x34390182
Hash Algorithm: sha256
md5: ef2a75096b68cf440939000240daa8db
sha1: 47e55e1c612d1ec7c77f705bb53bd469e5e8075e
sha256: 682f3e18ea60b3048a7e6aba8e5072e00368585a30ce4e23ce1c5c68a3f13aeb
sha512: 24f57fe68ad798cc8b6fb685fb311f24412001e0324f672465a357297b544fcdd7766008a7cd5be8f5115744c1d4ff41216a1b7bcfa90c1ffbdb3047b0649368
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 644d250903e6a21a1762f5c290b4a4b1b9e9c7571166d9583cd661cfb9a0f263
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
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.

APKID ANALYSIS

FILE	DETAILS
classes.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.TAGS check network operator name check ro.kernel.qemu check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.lowestmed.android.MainActivity	Schemes: https://, rxsaver://, Hosts: rxsaver.onelink.me,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: 0 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.

CODE ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/a/a/a/k0/m.java com/appsflyer/AFLogger.java com/segment/analytics/AnalyticsActivityLifecycleCallbacks.java f/c/a/b/e/e.java f/c/a/b/f/n/k.java f/c/a/e/b/a.java f/c/a/e/c/a.java f/c/a/e/f/c/b.java f/c/a/e/f/c/e.java f/c/a/e/f/c/j.java f/c/a/e/f/c/k.java f/c/a/e/f/c/l.java f/c/a/e/f/c/p4.java f/c/a/e/f/e/i0.java f/c/a/e/f/e/j.java f/c/a/e/f/e/o.java f/c/a/e/f/e/s.java f/c/a/e/f/e/t.java f/c/a/e/f/f/b.java f/c/a/e/f/g/n.java f/c/a/e/f/h/a3.java f/c/a/e/f/h/d2.java f/c/a/e/f/h/f2.java f/c/a/e/f/h/g.java f/c/a/e/f/h/g2.java f/c/a/e/f/h/i2.java f/c/a/e/f/h/j.java f/c/a/e/f/h/j2.java f/c/a/e/f/h/t1.java f/c/a/e/f/h/t3.java f/c/a/e/f/h/vb.java f/c/a/e/f/h/w1.java f/c/a/e/f/h/z.java f/c/a/e/h/b/h9.java f/c/a/e/h/b/r3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/c/a/e/h/b/v4.java f/c/a/e/j/b/a.java f/c/a/e/k/a.java f/c/a/e/k/b.java f/c/b/c.java f/c/b/h/e/b.java f/c/b/h/e/e.java f/c/b/h/e/g.java f/c/b/h/e/h.java f/c/b/h/e/k/a0.java f/c/b/h/e/k/g.java f/c/b/h/e/k/h0.java f/c/b/h/e/k/m0.java f/c/b/h/e/k/n.java f/c/b/h/e/k/n0.java f/c/b/h/e/k/q0.java f/c/b/h/e/k/u.java f/c/b/h/e/k/w0.java f/c/b/h/e/l/e.java f/c/b/h/e/q/b.java f/c/b/h/e/q/d/c.java f/c/b/h/e/s/a.java f/c/b/h/e/s/c.java f/c/b/h/e/s/d.java f/c/b/h/e/s/j/a.java f/c/b/l/b0.java f/c/b/l/d.java f/c/b/l/h.java f/c/b/l/i.java f/c/b/l/j.java f/c/b/l/k.java f/c/b/l/m0.java f/c/b/l/n0.java f/c/b/l/p.java f/c/b/l/q.java f/c/b/l/r.java f/c/b/l/s.java f/c/b/l/s0.java f/c/b/l/t.java f/c/b/l/u.java f/c/b/l/v.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	f/c/b/l/x.java f/c/b/z.java f/c/b/n/a.java f/c/b/n/d.java f/c/b/n/k/b.java f/c/b/n/l/c.java f/c/b/p/a.java f/c/b/p/b/a.java f/c/b/p/b/c.java f/c/b/p/b/d.java f/c/b/p/b/e.java f/c/b/p/b/f.java f/c/b/p/b/g.java f/c/b/p/b/h.java f/c/b/p/b/k.java f/c/b/p/b/l.java f/c/b/p/b/t.java f/c/b/p/d/d.java f/c/b/r/f.java f/c/b/r/j.java f/c/b/r/l/k.java f/c/b/r/l/o.java f/d/android/coupon/j.java f/e/a/k0/f.java i/b/c/g.java i/b/c/i.java i/b/c/p.java i/b/c/s.java i/b/g/e.java i/b/h/c.java i/b/h/d0.java i/b/h/f.java i/b/h/s.java i/b/h/v.java i/b/h/w.java i/f/a/a/c.java i/f/a/b/c.java i/f/a/b/e.java i/f/a/b/f.java i/f/a/b/g.java i/f/a/b/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				i/f/a/b/j.java i/f/a/b/k.java i/f/a/b/l.java i/f/a/b/m.java i/f/a/b/q.java i/f/a/b/r.java i/f/a/b/s.java i/f/b/d.java i/f/c/a.java i/f/c/b.java i/f/c/g.java i/h/b/c.java i/h/b/n.java i/h/c/b/e.java i/h/d/c.java i/h/j/a.java i/h/j/k.java i/i/a/b.java i/m/b/a.java i/m/b/a0.java i/m/b/b.java i/m/b/m0.java i/m/b/n0.java i/m/b/u.java i/m/b/x.java i/m/b/z.java i/r/b.java i/r/y/a.java i/room/InvalidationTracker.java i/room/MultiInstanceInvalidationClient.java i/room/RoomDatabase.java i/room/RoomOpenHelper.java i/room/SQLiteCopyOpenHelper.java i/t/b.java i/x/db/SupportSQLiteOpenHelper.java i/x/db/framework/FrameworkSQLiteOpenHelper.java i/x/util/ProcessLock.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p/a/e/f.java
2	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	f/c/a/b/f/p/i/t.java f/c/a/b/f/p/i/z.java f/c/a/e/b/a.java f/c/a/e/h/b/ca.java f/c/a/e/h/b/d.java f/c/a/e/h/b/h9.java f/c/a/e/h/b/n3.java f/c/a/e/h/b/x9.java i/x/db/framework/FrameworkSQLiteDatabase.java
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/appsflyer/internal/af.java f/c/b/h/e/k/g.java f/c/b/l/j.java f/c/b/n/k/b.java f/c/b/p/b/r.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	f/c/a/e/h/b/v4.java f/c/b/h/e/k/g.java
5	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/appsflyer/internal/a.java f/c/a/e/h/b/u9.java f/c/b/f/b.java f/c/b/r/j.java f/c/b/r/l/j.java
6	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	f/c/b/n/k/c.java i/room/SQLiteCopyOpenHelper.java
7	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	com/appsflyer/internal/af.java f/c/a/e/h/b/u9.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/appsflyer/AppsFlyerProperties.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/lowestmed/android/App.java f/c/a/e/h/b/v4.java f/c/b/h/e/k/u.java f/c/b/h/e/o/g.java f/c/b/h/e/s/a.java f/c/b/l/n0.java f/c/b/n/k/c.java f/c/b/r/j.java f/c/b/r/l/e.java i/room/SQLiteCopyOpenHelper.java i/room/util/a.java okio/Okio__JvmOkioKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/ae.java com/appsflyer/internal/j.java com/appsflyer/share/CrossPromotionHelper.java com/lowestmed/android/MainActivity.java com/lowestmed/android/coupon/CouponFragment.java com/lowestmed/android/priceListView/PriceListViewFragment.java com/lowestmed/android/settings/SettingsWebviewFragment.java f/c/a/e/h/b/d7.java f/d/android/somethingWentWrong/a.java f/d/android/somethingWentWrong/b.java i/r/b.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/lowestmed/android/coupon/CouponFragment.java com/lowestmed/android/priceListView/PriceListViewFragment.java com/lowestmed/android/settings/SettingsWebviewFragment.java f/d/android/somethingWentWrong/a.java f/d/android/somethingWentWrong/b.java i/r/b.java
00022	Open a file from given absolute path of the file	file	com/appsflyer/internal/ae.java i/room/SQLiteCopyOpenHelper.java i/x/db/framework/FrameworkSQLiteOpenHelper.java i/x/util/ProcessLock.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/ae.java com/appsflyer/internal/ay.java com/appsflyer/internal/m.java f/c/a/b/e/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/ae.java f/c/a/b/e/c.java f/c/a/e/h/b/b7.java f/c/a/e/h/b/u3.java f/c/b/n/l/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/ae.java com/appsflyer/internal/ay.java com/appsflyer/internal/j.java com/appsflyer/internal/m.java com/appsflyer/share/CrossPromotionHelper.java f/c/a/b/e/c.java f/c/b/n/l/c.java
00094	Connect to a URL and read data from it	command network	f/c/a/e/h/b/b7.java f/c/a/e/h/b/u3.java
00108	Read the input stream from given URL	network command	f/c/a/e/h/b/b7.java f/c/a/e/h/b/u3.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	f/c/a/e/f/c/b5.java f/c/a/e/f/e/z.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/ah.java com/appsflyer/internal/br.java com/appsflyer/internal/bw.java f/c/a/e/f/c/b5.java f/c/a/e/f/e/z.java
00187	Query a URI and check the result	collection sms calllog calendar	f/c/a/e/f/c/b.java f/c/a/e/f/c/b5.java f/c/a/e/f/e/z.java f/c/a/e/f/h/t1.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/ae.java com/appsflyer/internal/j.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/ae.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	com/appsflyer/internal/ae.java
00004	Get filename and put it to JSON object	file collection	com/appsflyer/internal/ae.java
00125	Check if the given file path exist	file	com/appsflyer/internal/ae.java
00153	Send binary data over HTTP	http	com/appsflyer/internal/ae.java
00016	Get location info of the device and put it to JSON object	location collection	com/appsflyer/internal/ae.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/ae.java com/appsflyer/internal/aq.java com/appsflyer/internal/br.java com/appsflyer/share/CrossPromotionHelper.java com/lowestmed/android/coupon/CouponFragment.java i/b/h/v.java i/r/b.java
00123	Save the response to JSON after connecting to the remote server	network command	com/appsflyer/internal/ay.java com/appsflyer/internal/m.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/ay.java com/appsflyer/internal/m.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/y.java f/e/a/g.java
00075	Get location of the device	collection location	i/b/c/s.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/ah.java com/appsflyer/internal/bw.java i/b/h/v.java
00014	Read file into a stream and put it into a JSON object	file	f/c/b/n/k/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/ah.java com/appsflyer/internal/br.java com/appsflyer/internal/bw.java f/c/a/e/f/h/w1.java
00046	Method reflection	reflection	f/d/android/coupon/j.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/ah.java com/appsflyer/internal/bw.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/ah.java com/appsflyer/internal/bw.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/ah.java com/appsflyer/internal/bw.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/ah.java com/appsflyer/internal/bw.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://rmn-rxsaver.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/569834841155/namespaces/firebase:fetch?key=AIzaSyAra-zlDkDFky7qoJkZwbmhNYfhqnc89E0 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'algolia_app_id': '7IG0ETFRXQ', 'algolia_index_name': 'rx-dev-drug-data-prod', 'algolia_search_api_key': '7c4ef1e882e0c72386df5cb5eff00bb0', 'december_quick_wins_enabled': 'true', 'dosage_details_prompt_enabled': 'true', 'e_psychiatry_ad_enabled': 'true', 'empty_saved_meds_search_cta_enabled': 'true', 'min_supported_version': '4.3.9', 'remote_config_cache_time_seconds': '7200', 'v3_api_enabled': 'true'}, 'state': 'UPDATE', 'templateVersion': '693'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, 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
www.googleadservices.com	ok	**IP:** 142.250.217.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
rmn-rxsaver.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
reports.crashlytics.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.goodrx.com	ok	**IP:** 151.101.130.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
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
www.e-psychiatry.com	ok	**IP:** 35.233.242.151 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
www.google.com	ok	**IP:** 142.250.72.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
update.crashlytics.com	ok	**IP:** 142.250.72.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
segment-api.rxsaver.com	ok	**IP:** 151.101.194.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
app-measurement.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
sregister.s	ok	No Geolocation information available.
api.rxsaver.com	ok	**IP:** 104.18.26.177 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cdn-settings.segment.com	ok	**IP:** 18.238.93.145 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
ktor.io	ok	**IP:** 13.224.53.49 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
rxsaver.com	ok	**IP:** 104.18.26.177 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
www.rxsaver.com	ok	**IP:** 104.18.12.163 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
goo.gl	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
support@rxsaver.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://rmn-rxsaver.firebaseio.com"
"google_api_key" : "AIzaSyAra-zlDkDFky7qoJkZwbmhNYfhqnc89E0"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAra-zlDkDFky7qoJkZwbmhNYfhqnc89E0"
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
70455870047544e590dbc111200fea96
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
d80f04be-b1ff-4830-8a1c-dc387be0aae7
M7GwBq0Ieh6dKTDWCs7om8JgfaW82ywJ
2943cd139cfa5679f649beaddd9fdc21
7c4ef1e882e0c72386df5cb5eff00bb0
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

PLAYSTORE INFORMATION

Title: RxSaver – Prescription Coupons

Score: 4.6326723 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.lowestmed.android

Developer Details: RxSaver, Inc., RxSaver,+Inc., None, https://www.rxsaver.com/, support@rxsaver.com,

Release Date: Jan 20, 2012 **Privacy Policy:** Privacy link

Description:

It’s your medication, only cheaper. RxSaver™ lets you search for your prescription drug in seconds and finds you the cheapest prices at nearby pharmacies, so there are no surprises at the pharmacy counter. RxSaver is free to use. No membership or sign in required. Whether you have insurance or not, you could be saving on your Rx medications. Using RxSaver is as easy as 1-2-3. 1. Enter your medication in the app 2. Get free Rx coupons to use at your pharmacy 3. Celebrate your savings. You’re now an RxSaver! Where is RxSaver Accepted? RxSaver coupons are accepted at all major U.S. pharmacies including: Walgreens, Walmart, CVS, Costco, Rite Aid, Kmart, Sam’s Club, Kroger, Duane Reade, HEB, Meijer, Publix, Randall’s, Safeway, and more. No matter where you fill your prescription, RxSaver can help you get good savings off the retail price of your Rx medication. How Much Does RxSaver Cost? RxSaver is free to use. There are no membership fees or sign in required. How Does the RxSaver App Work? It’s simple and easy. Just install the app, search for your prescription medication, edit the dosage as needed, and get the coupon you want. Using the “Save Med” button you can keep your rx medication information handy for quick price checks anytime. Can I Use Rx Coupons With Insurance or Without Insurance? RxSaver can be used by anyone who is insured, underinsured, or without insurance coverage. If the RxSaver coupon offers a better price than your health care insurance copay, simply use the coupon instead of your insurance for the prescription. Lower your out-of-pocket costs and feel good about your Rx savings. RxSaver is NOT INSURANCE. RxSaver coupons cannot be combined with federal/state-funded health care programs like Medicaid or Medicare. Can I use RxSaver at the pharmacy drive-thru? What about delivery? RxSaver is your single savings solution for home delivery, drive-thru, and pick-up from your local pharmacy. Just call ahead to give the pharmacist the coupon information over the phone, or read the codes at the drive-thru. RxSaver also allows you to compare drug prices between local and online pharmacies with free home delivery. Do RxSaver Coupons Work on Refills? Good news, RxSaver coupons never expire and you can keep the coupon on file at the pharmacy for all your refills. However, prescription prices can change over time. Searching for your medication through the RxSaver app is the best way to see current coupon prices. How is the RxSaver App Different from Rx Discount Cards? Paper Rx discount cards can get lost, but the RxSaver app is always free and easy to access on your device. The RxSaver app is a digital rx discount card that is always available when you need it and is the single easiest way to save at the pharmacy. The RxSaver app offers instant rx coupons on demand. Does RxSaver Work For Rx Pet Meds? If your pet needs prescription drugs, you don’t have to pay full-price! RxSaver offers free coupons for pet meds that have human equivalents, which can be easily filled at local pharmacies. Ask your vet before filling your pet's next prescription. Please visit https://www.goodrx.com/consumer-health-data-privacy-notice to read our Consumer Health Data Privacy Notice for additional information about our handling of consumer health data.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 01:43:25	Generating Hashes	OK

2025-08-31 01:43:25	Extracting APK	OK
2025-08-31 01:43:25	Unzipping	OK
2025-08-31 01:43:25	Parsing APK with androguard	OK
2025-08-31 01:43:25	Extracting APK features using aapt/aapt2	OK
2025-08-31 01:43:25	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 01:43:27	Parsing AndroidManifest.xml	OK
2025-08-31 01:43:27	Extracting Manifest Data	OK
2025-08-31 01:43:27	Manifest Analysis Started	OK
2025-08-31 01:43:28	Performing Static Analysis on: RxSaver (com.lowestmed.android)	OK
2025-08-31 01:43:29	Fetching Details from Play Store: com.lowestmed.android	OK
2025-08-31 01:43:31	Checking for Malware Permissions	OK

2025-08-31 01:43:31	Fetching icon path	OK
2025-08-31 01:43:31	Library Binary Analysis Started	OK
2025-08-31 01:43:31	Reading Code Signing Certificate	OK
2025-08-31 01:43:32	Running APKiD 2.1.5	OK
2025-08-31 01:43:35	Detecting Trackers	OK
2025-08-31 01:43:37	Decompiling APK to Java with JADX	OK
2025-08-31 01:43:51	Converting DEX to Smali	OK
2025-08-31 01:43:51	Code Analysis Started on - java_source	OK
2025-08-31 01:43:53	Android SBOM Analysis Completed	OK
2025-08-31 01:43:59	Android SAST Completed	OK

2025-08-31 01:43:59	Android API Analysis Started	OK
2025-08-31 01:44:06	Android API Analysis Completed	OK
2025-08-31 01:44:06	Android Permission Mapping Started	OK
2025-08-31 01:44:13	Android Permission Mapping Completed	OK
2025-08-31 01:44:14	Android Behaviour Analysis Started	OK
2025-08-31 01:44:22	Android Behaviour Analysis Completed	OK
2025-08-31 01:44:22	Extracting Emails and URLs from Source Code	OK
2025-08-31 01:44:24	Email and URL Extraction Completed	OK
2025-08-31 01:44:24	Extracting String data from APK	OK
2025-08-31 01:44:24	Extracting String data from Code	OK
2025-08-31 01:44:24	Extracting String values and entropies from Code	OK

2025-08-31 01:44:26	Performing Malware check on extracted domains	OK
2025-08-31 01:44:30	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.