MOBSF

ANDROID STATIC ANALYSIS REPORT

VA Rx Refill (4.5.0)

File Name:	com.rxr.production_76.apk
Package Name:	com.rxr.production
Scan Date:	Sept. 1, 2025, 8:26 a.m.
App Security Score:	62/100 (LOW RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	9	1	3	1

FILE INFORMATION

File Name: com.rxr.production_76.apk
Size: 7.27MB
MD5: 120350dbaa55ff40a56326f5821bdb42
SHA1: 3c69321b737940762849e26763042f84b5c86265
SHA256: 80bf493e56d76dd51ed257e7615f7e847f36d564ef8ec97a6de9f16ab1d3e0ce

APP INFORMATION

App Name: VA Rx Refill
Package Name: com.rxr.production
Main Activity: com.zoontek.rnbootsplash.RNBootSplashActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 4.5.0
Android Version Code: 76

APP COMPONENTS

Activities: 5
Services: 5
Receivers: 5
Providers: 3
Exported Activities: 1
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-10-28 20:53:57+00:00
Valid To: 2049-10-28 20:53:57+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x19967e896fba9c4e3d2190de7899dcbe11522093
Hash Algorithm: sha256
md5: 3d980aefca609ad18943bd8b4f38606e
sha1: ff2b992e4d62ec5558e7292a90030849b9e7590b
sha256: 031d3db54dbc1096f7e57fc49f23a8bc5a1982acf9166e5c27209252f1d86521
sha512: 6acf2caed9efb43acf9359dca1ebbb880565da7b09d940642ecb664c6d4292e9adc29eec8e8546e80ca826c3fe80353ad056b809589dd12fbbe235cdb3b823d8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2acd2486f55a56fd409316b5e2d8c2e202687531266eaa71dc71eeb9a4f12b16
Found 1 unique certificates

APPLICATION PERMISSIONS

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

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<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 SIM operator check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	Activity (com.rxr.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.
3	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal 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: **5** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a8/e.java a8/m.java b0/b.java b0/b0.java b0/h.java b0/r.java b0/s.java b0/u.java b7/b.java b7/c.java bd/c.java c0/c.java ca/b.java com/dieam/reactnativepushnotification/mo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/c.java com/lugg/RNCConfig/RNCConfigModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/a.java com/lwansbrough/RCTCamera/b.java com/lwansbrough/RCTCamera/e.java com/oblador/keychain/KeychainModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/webview/RNCWebViewModule.java com/sensors/RNSensor.java com/swmansion/gesturehandler/react/g.java com/swmansion/gesturehandler/react/h.java com/swmansion/reanimated/NativeProxy.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/b.java com/swmansion/reanimated/nodes/i.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/g.java d1/a.java d1/b.java d1/c.java d1/d.java da/c.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	e/a.java e8/b.java f0/c.java f7/k.java fc/g.java gc/b.java h0/a.java h4/f.java h7/a.java h9/d.java i/g.java i9/b.java j/c.java j8/o.java ld/c.java o9/i.java oa/k.java oa/m.java p0/a.java q/c.java q/g.java q/p.java q0/k.java q0/q0.java q9/c.java qa/c.java r/a.java r/b.java r/f.java r7/b.java r7/d.java r7/e.java r7/i.java r7/j.java r7/s.java r7/u.java r7/v.java r8/a.java s/c.java s/e.java s/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s/g.java s/k.java s7/d.java s7/g.java s7/h.java s7/k.java s7/r.java s7/v.java s8/a.java s9/g.java s9/n.java sa/a.java sa/j.java sb/a.java t/a.java t/e.java u7/a0.java u7/e.java u7/m0.java u7/x.java u7/z.java ua/b.java ua/c.java ub/b.java ub/g.java ub/h.java ub/i.java v1/g.java v7/a.java v7/b0.java v7/c.java v7/c1.java v7/d0.java v7/f1.java v7/i.java v7/p0.java v7/s0.java v7/t0.java v7/u0.java v7/w0.java v8/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				vb/c.java vb/f.java x/j.java x4/d.java xc/c.java xd/a.java z7/a.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	kd/c.java kd/d.java kd/g.java kd/h.java
3	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	c3/a.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java m3/a.java
4	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	c3/a.java ca/c.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/reactnativecommunity/webview/RNCWebViewModule.java h0/a.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/e.java l7/b0.java l7/f0.java l7/h0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	ad/b0.java od/d.java od/h.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ca/b.java p3/c.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	o9/w.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	d1/c.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java v7/i1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/reactnativecommunity/toolbarandroid/b.java d1/c.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java me/leolin/shortcutbadger/impl/a.java y6/a.java yc/b.java yc/c.java
00183	Get current camera parameters and change the setting.	camera	b7/b.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/b.java com/lwansbrough/RCTCamera/e.java
00013	Read file and put it into a stream	file	a3/b.java ca/c.java com/lwansbrough/RCTCamera/RCTCameraModule.java h0/a.java n5/e.java pd/r.java s/e.java s/k.java
00022	Open a file from given absolute path of the file	file	c3/f.java com/lwansbrough/RCTCamera/RCTCameraModule.java com/lwansbrough/RCTCamera/a.java com/oblador/vectoricons/a.java g3/c.java h0/a.java m3/a.java ud/h.java
00002	Open the camera and take picture	camera	b7/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00199	Stop recording and release recording resources	record	b7/b.java b7/c.java com/lwansbrough/RCTCamera/RCTCameraModule.java
00198	Initialize the recorder and start recording	record	b7/b.java b7/c.java com/lwansbrough/RCTCamera/RCTCameraModule.java
00194	Set the audio source (MIC) and recorded file format	record	b7/b.java b7/c.java
00197	Set the audio encoder and initialize the recorder	record	b7/b.java b7/c.java
00196	Set the recorded file format and output path	record file	b7/b.java b7/c.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java
00175	Get notification manager and cancel notifications	notification	d1/c.java
00114	Create a secure socket connection to the proxy address	network command	fd/f.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	ud/h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	c0/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	kd/b.java kd/h.java
00163	Create new Socket and connecting to it	socket	kd/b.java kd/h.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	v7/i1.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/a.java p3/f.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/a.java p3/f.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/a.java p3/f.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/a.java p3/f.java
00091	Retrieve data from broadcast	collection	com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/a.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/a.java
00014	Read file into a stream and put it into a JSON object	file	ca/c.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/c.java
00096	Connect to a URL and set request method	command network	da/c.java
00089	Connect to a URL and receive input stream from the server	command network	da/c.java
00109	Connect to a URL and get the response code	network command	da/c.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00195	Set the output path of the recorded file	record file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00007	Use absolute path of directory for the output media file path	file	com/lwansbrough/RCTCamera/RCTCameraModule.java
00041	Save recorded audio/video to file	record	com/lwansbrough/RCTCamera/RCTCameraModule.java
00012	Read data and put it into a buffer stream	file	h0/a.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.useplus.org	ok	**IP:** 54.83.4.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.npes.org	ok	**IP:** 172.67.183.61 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
purl.org	ok	**IP:** 207.241.225.157 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
veteran.apps.va.gov	ok	**IP:** 152.130.96.36 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.903450 **Longitude:** -77.027641 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
javax.xml.xmlconstants	ok	No Geolocation information available.
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
iptc.org	ok	**IP:** 3.64.29.21 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xerces.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cipa.jp	ok	**IP:** 118.82.81.189 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.aiim.org	ok	**IP:** 199.60.103.225 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	s7/q.java

HARDCODED SECRETS

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:26:18	Generating Hashes	OK
2025-09-01 08:26:18	Extracting APK	OK
2025-09-01 08:26:18	Unzipping	OK

2025-09-01 08:26:19	Parsing APK with androguard	OK
2025-09-01 08:26:19	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:26:19	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:26:20	Parsing AndroidManifest.xml	OK
2025-09-01 08:26:20	Extracting Manifest Data	OK
2025-09-01 08:26:20	Manifest Analysis Started	OK
2025-09-01 08:26:20	Performing Static Analysis on: VA Rx Refill (com.rxr.production)	OK
2025-09-01 08:26:22	Fetching Details from Play Store: com.rxr.production	OK
2025-09-01 08:26:23	Checking for Malware Permissions	OK
2025-09-01 08:26:23	Fetching icon path	OK

2025-09-01 08:26:23	Library Binary Analysis Started	OK
2025-09-01 08:26:23	Reading Code Signing Certificate	OK
2025-09-01 08:26:24	Running APKiD 2.1.5	OK
2025-09-01 08:26:26	Detecting Trackers	OK
2025-09-01 08:26:27	Decompiling APK to Java with JADX	OK
2025-09-01 08:26:36	Converting DEX to Smali	OK
2025-09-01 08:26:36	Code Analysis Started on - java_source	OK
2025-09-01 08:26:38	Android SBOM Analysis Completed	OK
2025-09-01 08:26:44	Android SAST Completed	OK
2025-09-01 08:26:44	Android API Analysis Started	OK

2025-09-01 08:26:49	Android API Analysis Completed	OK
2025-09-01 08:26:49	Android Permission Mapping Started	OK
2025-09-01 08:26:55	Android Permission Mapping Completed	OK
2025-09-01 08:26:55	Android Behaviour Analysis Started	OK
2025-09-01 08:27:02	Android Behaviour Analysis Completed	OK
2025-09-01 08:27:02	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:27:03	Email and URL Extraction Completed	OK
2025-09-01 08:27:03	Extracting String data from APK	OK
2025-09-01 08:27:03	Extracting String data from Code	OK
2025-09-01 08:27:03	Extracting String values and entropies from Code	OK
2025-09-01 08:27:04	Performing Malware check on extracted domains	OK

2025-09-01 08:27:06	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.