MOBSF

ANDROID STATIC ANALYSIS REPORT

GoodRx (8.35.1)

File Name:	com.goodrx_442.apk
Package Name:	com.goodrx
Scan Date:	Aug. 29, 2025, 11:09 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	25	4	3	2

FILE INFORMATION

File Name: com.goodrx_442.apk
Size: 55.0MB
MD5: 82ef2b903bd2005f621d8b264dda3fdf
SHA1: 529973625e22b9b699c2dd653c8400c64848cf0c
SHA256: f3d597349ad4ccc85055b4fb4fb98abb2c02e8ae799702a299fbe744beadce6d

APP INFORMATION

App Name: GoodRx
Package Name: com.goodrx
Main Activity: com.goodrx.splash.ui.SplashActivity
Target SDK: 35
Min SDK: 26
Max SDK:
Android Version Name: 8.35.1

Android Version Code: 442

APP COMPONENTS

Activities: 51
Services: 21
Receivers: 19
Providers: 8
Exported Activities: 7
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=CA, L=Santa Monica, O=GoodRx Inc, CN=Billy McClure
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-12-09 01:25:19+00:00
Valid To: 2037-12-03 01:25:19+00:00
Issuer: C=US, ST=CA, L=Santa Monica, O=GoodRx Inc, CN=Billy McClure
Serial Number: 0x50c3e87f
Hash Algorithm: sha1
md5: e0a6e898ab70a75bed2a8ca880f88d7e
sha1: 1ab4e1435c904d1dd221de9f9ed0c39c72de0b81
sha256: 368b60034507f72bf19c51abfeb3d43b7b1c25e8986fdbeb0443802d1b7492c8
sha512: 0b474190ef07ae31759678c09aec468e4afb162ace2f96f8ce5af62203263394a23aba8fea1ec4582689b3cbfc728a4ce2d0ace71b6beab1d3b58840364de5b0
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 487d661dee8375bcfb1a30bec89266ab88597df1ada229068a995a44424e6c71
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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

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.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.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.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.goodrx.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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_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.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.

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.goodrx.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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 Build.TAGS check network operator name check ro.kernel.qemu check</td></tr><tr><td>Compiler</td><td>dexlib 1.x r8 without marker (suspicious)</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>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.MANUFACTURER check</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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes5.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.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check network operator name check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.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.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes7.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.goodrx.splash.ui.SplashActivity	Schemes: http://, https://, goodrx://, Hosts: www.goodrx.com, Path Prefixes: /li,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.goodrx,

ACTIVITY	INTENT
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.goodrx,
com.auth0.android.provider.RedirectActivity	Schemes: @string/com_auth0_scheme://, Hosts: @string/com_auth0_domain, Path Prefixes: /android/com.goodrx/callback,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: 0 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	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	Broadcast Receiver (com.google.ads.conversiontracking.InstallReceiver) 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.
3	Activity (com.goodrx.main.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.
4	Activity (com.goodrx.licenses.LicenseActivity) 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.
5	Broadcast Receiver (com.goodrx.consumer.feature.home.data.workers.DailyMedReminderNotificationBroadcastReciever) 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
6	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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.
7	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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	TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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
11	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.
12	Activity (com.airbnb.android.showkase.ui.ShowkaseBrowserActivity) 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.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Activity (com.auth0.android.provider.RedirectActivity) 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.
15	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.

NO	ISSUE	SEVERITY	DESCRIPTION
16	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: **3** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	B1/C3103r0.java B4/c.java B4/h.java Hm/a.java J1/D.java Uf/C3731y.java com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java com/fasterxml/uuid/a.java com/fasterxml/uuid/b.java com/fasterxml/uuid/g.java j$/util/concurrent/ThreadLocalRandom.java o4/C13503a.java
				B2/d.java B7/e.java B7/l.java Fg/C3191e.java Fj/f.java He/f.java I2/c.java Ke/RemoteMessagePayload.java Kk/PopupPayload.java Mn/C3417d0.java P2/c.java U6/a.java ac/C3919h.java ac/DeepLinkObject.java com/affirm/android/AffirmConstants.java com/affirm/android/model/C$$AutoValue_Merchant.java com/datadog/android/rum/internal/domain/scope/e.java com/datadog/android/rum/internal/domain/scope/k.java com/goodrx/common/core/ui/price/pharmacy

NO	ISSUE	SEVERITY	STANDARDS	FILES
				SavingsModule/ui/u.java com/goodrx/common/feature/account/ui/A.java com/goodrx/consumer/feature/coupon/ui/coupon/InterfaceC5383a.java com/goodrx/consumer/feature/ecom/usecase/e.java com/goodrx/consumer/feature/gold/ui/goldCard/goldCardPage/b.java com/goodrx/consumer/feature/gold/ui/goldCard/goldCardPage/d.java com/goodrx/consumer/feature/gold/ui/goldCouponPage/InterfaceC5498b.java com/goodrx/consumer/feature/gold/ui/goldCouponPage/InterfaceC5512p.java com/goodrx/consumer/feature/gold/ui/goldPriceProtection/gPPWelcomeBottomSheet/a.java com/goodrx/consumer/feature/gold/ui/goldPriceProtection/gPPWelcomeBottomSheet/j.java com/goodrx/consumer/feature/gold/ui/homeDelivery/activeOrderBottomSheet/f.java com/goodrx/consumer/feature/gold/ui/homeDelivery/verifyOrderBottomSheet/g.java com/goodrx/consumer/feature/gold/ui/registration/goldWelcomePage/a.java com/goodrx/consumer/feature/gold/ui/registration/goldWelcomePage/k.java com/goodrx/consumer/feature/gold/ui/registration/reenroll/I.java com/goodrx/consumer/feature/gold/usecase/H.java com/goodrx/consumer/feature/gold/usecase/J.java com/goodrx/consumer/feature/home/ui/details/prescription/gHDRxDetailsPage/d.java com/goodrx/consumer/feature/home/ui/details/prescription/h.java com/goodrx/consumer/feature/home/ui/healthContent/InterfaceC5681b.java com/goodrx/consumer/feature/home/ui/landi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ng/o.java com/goodrx/consumer/feature/home/ui/landing/p.java com/goodrx/consumer/feature/home/ui/resourcesForYou/m.java com/goodrx/consumer/feature/home/ui/resourcesForYou/p.java com/goodrx/consumer/feature/pharmacistentrymode/ui/c.java com/goodrx/consumer/feature/pharmacistentrymode/ui/k.java com/goodrx/consumer/feature/price/page/A1.java com/goodrx/consumer/feature/price/page/InterfaceC5869c.java com/goodrx/consumer/feature/rewards/ui/landing/i.java com/goodrx/consumer/feature/rewards/ui/landing/j.java com/goodrx/consumer/feature/selectpharmacy/ui/c.java com/goodrx/consumer/feature/testprofiles/view/environmentVars/i.java com/goodrx/consumer/feature/testprofiles/view/featuresAndExperiments/i.java com/goodrx/consumer/feature/testprofiles/view/testProfile/a.java com/goodrx/consumer/feature/testprofiles/view/testProfile/addSetting/a.java com/goodrx/consumer/feature/testprofiles/view/testProfile/overrideProfileCustomInput/a.java com/goodrx/consumer/feature/testprofiles/view/testProfile/overrideProfileCustomInput/v.java com/goodrx/consumer/feature/testprofiles/view/testProfile/overrideProfileProperty/b.java com/goodrx/consumer/feature/testprofiles/view/testProfile/overrideProfileProperty/j.java com/goodrx/consumer/feature/testprofiles/vi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ew/testProfile/overrideProfileProperty/l.java com/goodrx/consumer/feature/testprofiles/view/testProfile/v.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	com/goodrx/main/ui/a.java com/goodrx/platform/designsystem/component/dialog/r.java com/goodrx/platform/graphql/d.java com/optimizely/ab/config/Attribute.java com/optimizely/ab/config/DatafileProjectConfig.java com/optimizely/ab/config/EventType.java com/optimizely/ab/config/Experiment.java com/optimizely/ab/config/FeatureFlag.java com/optimizely/ab/config/FeatureVariable.java com/optimizely/ab/config/Integration.java com/optimizely/ab/config/Variation.java com/optimizely/ab/event/internal/payload/DecisionMetadata.java com/optimizely/ab/notification/i.java com/salesforce/marketingcloud/events/g.java com/salesforce/marketingcloud/events/h.java com/salesforce/marketingcloud/registration/Registration.java com/stripe/android/auth/PaymentBrowserAuthContract.java com/stripe/android/core/networking/j.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherContract.java com/stripe/android/model/C11298j.java com/stripe/android/model/C11299k.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/ConsumerSessionLookup.java com/stripe/android/model/ConsumerSessionSignup.java com/stripe/android/model/D.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/model/F.java com/stripe/android/model/H.java com/stripe/android/model/InterfaceC11310w.java com/stripe/android/model/O.java com/stripe/android/model/Q.java com/stripe/android/model/Source.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/X.java com/stripe/android/model/d0.java com/stripe/android/model/f0.java com/stripe/android/payments/bankaccount/navigation/CollectBankAccountContract.java com/stripe/android/payments/bankaccount/ui/a.java com/stripe/android/payments/c.java com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java com/stripe/android/payments/d.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract.java com/stripe/android/paymentsheet/N.java com/stripe/android/paymentsheet/O.java com/stripe/android/paymentsheet/PaymentSheetContract.java com/stripe/android/paymentsheet/S.java com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract.java com/stripe/android/paymentsheet/addresselement/h.java com/stripe/android/paymentsheet/paymentdatacollection/ach/g.java com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingContract.java com/stripe/android/paymentsheet/paymentdatacollection/polling/h.java com/stripe/android/paymentsheet/repositories/c.java com/stripe/android/paymentsheet/state/a.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a com/stripe/android/polling/c.java com/stripe/android/r.java com/stripe/android/stripe3ds2/transaction/B.java com/stripe/android/stripe3ds2/transaction/C11425a.java com/stripe/android/stripe3ds2/transaction/C11427c.java com/stripe/android/uicore/elements/AbstractC11501i.java ea/g.java f5/i.java gc/C11925r0.java gc/G2.java k5/C12660A.java o6/C13546q.java o8/C13584n.java q6/C14280H.java q6/C14300n.java q6/r.java q7/C14312a.java r5/d.java r5/h.java re/g.java sf/ModalCtaSelected.java sf/ModalViewed.java u8/g.java v4/C14851a.java v7/j.java v7/o.java xj/C15289d.java xj/f.java ya/AbstractC15360n.java ya/C15355i.java ya/C15364r.java z5/C15463a.java
				lf/M.java lf/U.java com/optimizely/ab/android/event_handler/e.java com/salesforce/marketingcloud/storage/db/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/salesforce/marketingcloud/storage/db/b.java com/salesforce/marketingcloud/storage/db/c.java com/salesforce/marketingcloud/storage/db/e.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/g.java com/salesforce/marketingcloud/storage/db/h.java com/salesforce/marketingcloud/storage/db/i.java com/salesforce/marketingcloud/storage/db/j.java com/salesforce/marketingcloud/storage/db/k.java com/salesforce/marketingcloud/storage/db/l.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/b.java com/salesforce/marketingcloud/storage/db/upgrades/c.java com/salesforce/marketingcloud/storage/db/upgrades/d.java com/salesforce/marketingcloud/storage/db/upgrades/e.java com/salesforce/marketingcloud/storage/db/upgrades/f.java com/salesforce/marketingcloud/storage/db/upgrades/g.java com/salesforce/marketingcloud/storage/db/upgrades/h.java com/salesforce/marketingcloud/storage/db/upgrades/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/salesforce/marketingcloud/storage/db/upgrades/j.java Ah/g.java Bf/k.java Bg/i.java Cg/d.java D0/f.java Di/n.java Di/p.java Do/j.java E/u.java Ef/a.java Eh/l.java Eh/m.java Ek/e.java Fg/C3196j.java G/d.java Gd/a.java Hl/C3293g.java Hl/C3295i.java Ig/l.java K4/a.java L0/d.java Mi/a.java Nh/a.java Nh/b.java Nh/c.java O0/t.java O1/l.java P1/g.java Qj/l.java R0/c.java Sg/w.java Sh/e.java Ti/a.java Ti/g.java Ug/AbstractC3742f.java Vg/P.java Vh/f.java Vh/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				W0/c.java Xf/b.java Yf/n.java Yg/a.java Z/c.java Z/g.java ah/C3948a.java ap/a.java b3/C5034c.java bh/C5071a.java com/affirm/android/Affirm.java com/affirm/android/AffirmFragment.java com/affirm/android/AffirmTrackView.java com/affirm/android/AffirmUtils.java com/affirm/android/AffirmWebViewClient.java com/affirm/android/CheckoutRequest.java com/affirm/android/PromotionWebView.java com/affirm/android/TrackerRequest.java com/apollographql/apollo/network/ws/c.java com/apollographql/apollo/network/ws/f.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/auth0/android/provider/AbstractC5244k.java com/auth0/android/provider/B.java com/auth0/android/provider/C5234a.java com/auth0/android/provider/C5240g.java com/auth0/android/provider/C5247n.java com/auth0/android/provider/O.java com/auth0/android/request/internal/JwksDeserializer.java com/datadog/android/rum/DdRumContentProvider.java com/datadog/android/rum/internal/domain/scope/m.java com/franmontiel/persistentcookiejar/persisten

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	ce/SerializableCookie.java com/goodrx/notifications/o.java com/goodrx/startup/a.java com/mikepenz/aboutlibraries/ui/compose/m3/t.java com/salesforce/marketingcloud/MCLogListener.java com/salesforce/marketingcloud/g.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/KeyStoreWrapper.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java com/salesforce/marketingcloud/sfmcsdk/components/logging/LogListener.java com/salesforce/marketingcloud/sfmcsdk/components/logging/Logger.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/stripe/android/stripe3ds2/transaction/D.java com/stripe/android/ui/core/elements/s0.java com/stripe/android/uicore/image/b.java com/stripe/hcaptcha/webview/HCaptchaWebView.java d1/C11560c.java dh/AbstractC11624b.java dh/P.java eh/C11710e.java ii/C12220b.java jh/C12559d.java ji/c.java k1/AbstractC12585a.java m/AbstractC13121a.java m/C13122b.java m2/n.java ng/g.java o3/C13501b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java org/slf4j/helpers/Util.java p2/AbstractC13849a.java pf/C14172a.java pg/AbstractC14173A.java pg/AbstractC14182b.java pg/C14176D.java pg/C14177E.java pg/C14183c.java pg/C14191k.java pg/ServiceConnectionC14204x.java pg/y.java q1/AbstractC14235c.java qg/z.java r1/C14393a.java r2/h.java rg/AbstractBinderC14462a.java rg/AbstractC14465c.java rg/C14472j.java rg/E.java rg/H.java rg/c0.java rg/f0.java rg/g0.java rg/h0.java rg/j0.java rg/p0.java rg/t0.java rj/C14493d.java s2/C14512a.java t0/C14609a.java t1/AbstractC14612a.java u/M.java u2/AbstractC14732b.java ug/C14824a.java w/K.java wf/AbstractC15071a.java x1/p.java xg/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xh/C15281d.java xh/d.java y0/d.java yg/g.java yg/s.java yg/t.java yh/b.java yi/j.java zd/a.java
5	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	com/affirm/android/VcnDisplayActivity.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	Sn/a.java Tn/a.java Un/a.java Vn/a.java dj/C11652a.java ko/e.java
7	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/salesforce/marketingcloud/sfmcsdk/components/encryption/EncryptedSharedPreferences.java
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/perimeterx/mobile_sdk/PerimeterX.java com/perimeterx/mobile_sdk/block/PXBlockActivity.java
9	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	ii/C12221c.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	Ni/a.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Lj/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java ii/C12220b.java
13	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	Yf/g.java com/salesforce/marketingcloud/util/l.java
14	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/affirm/android/AffirmUtils.java
15	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	lb/a.java bd/C5060a.java
16	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.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	Gd/a.java Hl/C3289c.java Kl/a.java Tf/t.java Tj/H.java Wf/C3804a.java bc/C5058b.java com/affirm/android/AffirmWebChromeClient.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/auth0/android/provider/C5243j.java com/auth0/android/provider/O.java com/goodrx/main/MainActivity.java com/goodrx/splash/ui/SplashActivity.java com/salesforce/marketingcloud/notifications/b.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/m.java com/stripe/android/ui/core/elements/AbstractC11447e.java com/stripe/android/uicore/text/c.java com/stripe/android/view/C11535i0.java com/stripe/android/view/C11537j0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	Hl/C3289c.java Oj/b.java Xf/F0.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/datadog/android/rum/l.java com/goodrx/consumer/feature/home/data/workers/DailyMedReminderNotificationBroadcastReciever.java com/salesforce/marketingcloud/alarms/b.java com/salesforce/marketingcloud/messages/push/a.java com/salesforce/marketingcloud/sfmcsdk/components/behaviors/BehaviorManagerImpl.java com/stripe/android/link/LinkForegroundActivity.java
00078	Get the network operator name	collection telephony	Hl/I.java Oj/b.java com/appsflyer/internal/AFh1cSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	Mi/a.java Qn/E0.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/datadog/android/core/internal/persistence/file/batch/e.java com/optimizely/ab/internal/k.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/salesforce/marketingcloud/util/e.java com/salesforce/marketingcloud/util/f.java com/salesforce/marketingcloud/util/g.java ii/C12221c.java okio/Okio__JvmOkioKt.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java p2/AbstractC13850b.java sj/C14583a.java z1/C15439c.java z1/u.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/stripe/android/payments/core/authentication/i.java com/stripe/android/stripe3ds2/transaction/I.java ji/c.java ng/f.java z1/C15447k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/salesforce/marketingcloud/storage/db/a.java com/salesforce/marketingcloud/storage/db/d.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/j.java
00034	Query the current data network type	collection network	Oj/b.java Xf/AbstractC3817c.java
00125	Check if the given file path exist	file	Oj/b.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/notifications/b.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/stripe/android/stripe3ds2/transaction/I.java ji/c.java sj/C14584b.java z1/C15447k.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFb1uSDK.java com/salesforce/marketingcloud/notifications/b.java com/stripe/android/stripe3ds2/transaction/I.java z1/C15447k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	Gd/a.java H2/e.java Hl/C3289c.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/auth0/android/provider/O.java com/goodrx/main/MainActivity.java com/salesforce/marketingcloud/notifications/b.java z1/u.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java com/stripe/android/core/networking/l.java com/stripe/android/stripe3ds2/transaction/l.java ji/c.java z1/C15447k.java
00028	Read file from assets directory	file	z1/C15437a.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1nSDK.java ii/C12221c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	Q2/i.java Qj/a.java coil/disk/a.java com/appsflyer/internal/AFg1nSDK.java com/datadog/android/core/internal/persistence/e.java com/datadog/android/ndk/internal/NdkCrashReportsFeature.java com/datadog/android/ndk/internal/c.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/util/e.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1nSDK.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java io/branch/coroutines/c.java
00161	Perform accessibility service action on accessibility node info	accessibility service	O0/t.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	O0/t.java
00016	Get location info of the device and put it to JSON object	location collection	com/salesforce/marketingcloud/messages/d.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java
00132	Query The ISO country code	telephony collection	x1/M.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Hl/C3289c.java Tf/t.java Wf/C3804a.java com/goodrx/main/MainActivity.java com/goodrx/splash/ui/SplashActivity.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/m.java com/stripe/android/uicore/text/c.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00024	Write file after Base64 decoding	reflection file	Q2/i.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java
00003	Put the compressed bitmap data into JSON object	camera	Il/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	w1/C14955a.java
00012	Read data and put it into a buffer stream	file	com/datadog/android/core/internal/persistence/file/batch/e.java
00202	Make a phone call	control	com/goodrx/main/MainActivity.java
00203	Put a phone number into an intent	control	com/goodrx/main/MainActivity.java
00094	Connect to a URL and read data from it	command network	z1/C15447k.java
00108	Read the input stream from given URL	network command	z1/C15447k.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://western-will-572.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/884942033917/namespaces/firebase:fetch?key=AIzaSyAACTFD57EXQsT9CN8dbuVVk7s9_E56nNM. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	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.VIBRATE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, 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
merchant-ui-api.stripe.com	ok	**IP:** 54.203.175.79 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
link.com	ok	**IP:** 35.166.203.173 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
help.branch.io	ok	**IP:** 104.18.21.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
privacy.abbvie	ok	**IP:** 104.18.41.239 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.stripe.com	ok	**IP:** 54.149.153.72 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
mcy4j9r6zlb680j9gcyj78x420-m.device.marketingcloudapis.com	ok	**IP:** 96.43.154.32 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
checkout.link.com	ok	**IP:** 151.101.192.176 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
npiregistry.cms.hhs.gov	ok	**IP:** 13.224.53.126 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
kids.nationalgeographic.com	ok	**IP:** 18.155.173.95 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
link.co	ok	**IP:** 13.224.53.115 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
manage.auth0.com	ok	**IP:** 104.18.39.72 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.igodigital.com	ok	**IP:** 3.218.154.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
perimeterx.net	ok	**IP:** 34.120.250.63 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
gql-activations-graph-00fa5616.sbx.uw2.eng.grxweb.com	ok	No Geolocation information available.
q.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
gx9e.app.link	ok	**IP:** 18.238.109.123 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
logx.optimizely.com	ok	**IP:** 34.49.241.189 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
r.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 64.233.177.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
googlemobileadssdk.page.link	ok	**IP:** 142.250.105.132 **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.
sars.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
g.co	ok	**IP:** 172.217.215.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.animalplanet.com	ok	**IP:** 18.155.173.57 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
western-will-572.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
salesforce-marketingcloud.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
static.afterpay.com	ok	**IP:** 104.16.223.179 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
lcn-prd-server.lifecycle.dev.goodrx.com	ok	**IP:** 15.197.202.126 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
docs.perimeterx.com	ok	**IP:** 35.241.52.23 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
ktor.io	ok	**IP:** 13.224.53.95 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
perimeterx.jfrog.io	ok	**IP:** 18.214.229.238 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.goodrx.com	ok	**IP:** 151.101.2.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
default.url	ok	No Geolocation information available.
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:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 64.233.176.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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.
www.grxstatic.com	ok	**IP:** 151.101.66.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.stripe.com	ok	**IP:** 52.24.225.18 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.example.com	ok	**IP:** 23.56.109.241 **Country:** France **Region:** Provence-Alpes-Cote-d'Azur **City:** Marseille **Latitude:** 43.296951 **Longitude:** 5.381070 **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
www.affirm.com	ok	**IP:** 162.159.140.33 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bnc.lt	ok	**IP:** 18.238.109.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.ipify.org	ok	**IP:** 104.26.12.205 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
cdn.branch.io	ok	**IP:** 18.238.109.61 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
gold.goodrx.coma	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
picsum.photos	ok	**IP:** 172.67.74.163 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
hooks.stripe.com	ok	**IP:** 54.191.201.88 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
gold.goodrx.com	ok	**IP:** 151.101.66.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
aomedia.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
support.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.rxabbvie.com	ok	**IP:** 18.238.109.42 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.253.124.102 **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.
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
errors.stripe.com	ok	**IP:** 198.202.176.111 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **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

DOMAIN	STATUS	GEOLOCATION
docs.stripe.com	ok	**IP:** 35.167.54.49 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
graph.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
scdn-ssettings.s	ok	No Geolocation information available.
www.affirm.ca	ok	**IP:** 162.159.140.33 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
gql-stitch-good-dev-0.lifecycle.dev.goodrx.com	ok	**IP:** 3.33.227.158 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.optimizely.com	ok	**IP:** 104.18.66.57 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.goodrx.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
support.stripe.com	ok	**IP:** 198.202.176.111 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	**IP:** 173.194.219.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-staging.goodrx.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
stage.app.igodigital.com	ok	**IP:** 52.3.169.193 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
images.ctfassets.net	ok	**IP:** 18.238.109.59 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stripe.com	ok	**IP:** 52.89.224.113 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
www.goodrx.com	ok	**IP:** 151.101.2.49 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
john.doe@goodrx.com	Z5/C3866a.java
support@stripe.com	zk/C15518a.java
test@goodrx.com	com/goodrx/consumer/feature/wallet/data/a.java
goldposfamilyannual2@mailinator.com	com/goodrx/consumer/feature/home/debug/c.java
info@goodrx.com	com/goodrx/main/navigation/v1.java
support@stripe.com	com/stripe/android/networking/f.java
support@stripe.com	com/stripe/android/core/networking/j.java
email@me.co	com/stripe/android/link/ui/inline/b.java
info@goodrx.com support@stripe.com support@goodrx.com email@address.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Optimizely	Analytics	https://reports.exodus-privacy.eu.org/trackers/172
Salesforce Marketing Cloud		https://reports.exodus-privacy.eu.org/trackers/220
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com_auth0_domain" : "auth.goodrx.com"
"com_auth0_scheme" : "https"
"consumer_feature_profile_auth0_complete_profile_finish" : "Finish"
"consumer_feature_profile_auth0_complete_profile_optional_label" : "Optional"
"firebase_database_url" : "https://western-will-572.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyAACTFD57EXQsT9CN8dbuVVk7s9_E56nNM"
"google_crash_reporting_api_key" : "AIzaSyAACTFD57EXQsT9CN8dbuVVk7s9_E56nNM"
"google_maps_key" : "AIzaSyAoZEE4jfFvwXYvi3gxDxyHKQLpm5BSwgY"
"platform_ads_api_ad" : "Ad"
"platform_auth_impl_skip" : "Skip"
323110dd6a31413b146ec0d4dadc3c6f70a0e7914cf5c29356b34f8da4e0e437
4feea7d897097b91de2de462a31b33d12086a711806b8574ece1e06e548749d0
41058363725152142129326129780047268409114441015993725554835256314039467401291
FlygBXZrpziR+Pp2xmzyZ9k6GUcrj9kWbY5XuUd40ERy2hxHTKqhUwfuGSusXUTd
F6389234-1024-481F-9173-37D9D7F5051F
b38aedc2-b600-452f-9950-c4bdfca96689
2301db94993b7737ea00d78be46ae79d3194541a182ea92c76f5dbf05667d3bc
81141880f17640fb40fef919564afe460769614ff1b4b130fe047a39b2779e0f
34d02886daf6283f8d841a50ba91c6107f0691151060b235480fdb92c9c8e7f0
d887cbf0f9e028a2ec32e9b57c37cfef1aa1d4f61e5adab55be04265725c1cf5

POSSIBLE SECRETS
5fbcdc65a51f5ddb99c040c0a84377074a026209e46581b2514e421bae4ed3d1
b164a60d849a01bd6d8fb5bae0c177d9f
013602400437880159360205O5
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
922cd2ef38a5fb19c095874e503680256dc3c79296ee22a40eb7db9cd9f5dd1c
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
cd0fa5bc868c2c0de2928d14cd7a1ddd947eea0c7e1c7333aa5a3aa66f683920
8HOKLqLOucCjn3kWyyKimNsF6Dcutdd9y3ap015kDIWZNsgYbLJqzHSzKo+jDSQ4
Gt05wIkB9VlCQDpYnwS+bvW/Sf4rdLdhAuNRhSCvQ2I=
3333cacd11f5b692f2fd6000de7f5c69ab05f331aad74d59cc929e417bd65113
3651d55822be48c473dab537670383142ce1ed00e0ca214fe47fe61794ce2c06
632649aa44ac770535c4cbaccefb59ceeb83d9fcbda56897a875106b4249678f
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
577af8d52f80c02adc208eb9d2692771c25a3c0a1331bfa91a45fd630d841c55

POSSIBLE SECRETS
c0efa4314d5f01f0eb6cd8a737d1ff2392248bdfe4445c59f406a92175cb50e6
1281c4d7d18d100fba88645cf8b35fe5e1250c7a62084d76708e84727460e2f1
pwlWlXowmv5MgDBY81mya6zXLrSMULDo97qGgXQvfFI=
skGQhdInPY4sBMicxMlDA8FpM67X6t386GsGM5hjG6o=
d82d330037fd1ab512aa169e8b8853e46180c3526843d5ceaaa56469010a97d1
qmKK3b5gFczPFV6EXQK4o/dThX0H+NXEfphwaNTcj5pJFkabLh1X9vORrSfnOkeV
0123456789abcdefABCDEF
953a7443c6c160e6f0119a0879869e63e7db90d110d37f9ac6da1d050fc36e95
c691eea62d104e33db2b682e1e026924438d2cadc63bf318c1c2e6fa5c36db5c
AjndXp1s5xIDXysf7TNVubDac7r00lcAtHKozpGmJzQ=
472e0ff73f86488bd6b9950e1d828a1f7289c30e456280ba4a719a3ac71adf26
8a62948c5764390dcc2d0bd99d7a7c7950dccb12bc686de905f648c8a40e1db9
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
uqJEUYtMC6igyTZFAAEE75NBgASQTYxYWvVnS4oyIqiXJPhpeFyV9nSFbcfeIJKd

POSSIBLE SECRETS
4aed48ff57a408d58b6e44e338a549310799cc3050c1363e18af913ba35f09ac
7c67cf9803e8c0fc9e1c3fc27359f984fa8d2f6998e8871ec0b621d9ed893867
1eASkBAriCqBxPWd4okyyc+CHCTvdkAuw8U5qBN0KobaC6TQVXZIuItjy1xo8n06
68b28e422d97c7c77b6e4eff126f126137dc0bbcdaae219ef8fd8492feded5ee
3fbb4da9-25c4-4966-9d5c-7cbf5609fde6
f59e8e558eb6398bc94df10306ccbc8d265da561c4cb383443ea15c1dc60108b
3ab29a6b8a4375f0a7e27b207130d69d
5UR6HKB81c0cBAmhqUCkwnSn0PivsbvOC36lSRnvbJazdJtsmM3DNCGH8hJ11MS9
5dbeb999f138413635c79f89d044bcae334983e70360a67de666787f1b0f062e
525ab0f741bcc0d660cc3ddd470f374785b188faa2a82c9b827c28641a8f332e
6756d1fe9bc9114721750a154c42782400c5061007c1e46ff6cf06af4be2945c
7b489e182aac5a8b8aaf5c55d5709e4771dc1f10f58791b3e321a1c17733d545
abd180536a6b80992f584e7b15cd77d7254aa90c212bcd8d1dc37275e8c3c9fc
b5bb2575f88a2f35dc0233deaf172b9dcfff37c3cb71d650588d561550d57268
aa317eb4774b4dcc317d5d0baa6c030be1e139c3233508ee27d8365f6e1623af

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
1fc2ad74a1487e703b27699be4c2e42fcb67ba85c936136b885c470e73f211d6
c0a9952d3c301f3e469d380149a6b9e319fe8a3a2793eb3e0cac2c43790eddfc
78211cd104affcdff807fe06085913b083aad041a8deb3d8499cfedd2606acf6
70a52c7825876979c3328fd5d646802a8c393aa09487fed771b945e8dfb3e245
UrsneQ7OIRNo8EjOO9YdieQqewqlcsXgRCgjv7EyHmQ=
5gR2Yi2k1qmqwB908rtZUebo4TzAbjEGSkWYIuNbRdnGPocO4kIxU9dsn2qP+c0J
af1c399ab120885c7766714c7d7d9ad1a9e568b1b29ff8fed10e05dc2b8353f3
da5cba5aab4be299d63ed4ec4c5014104e553116350811da90ea9ad490c3d11e
82807698c47e727b0b887d5b2dfb13fb413f0d760e5650d934a03d04b46409f3
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
c927b1c9a933b476e12b8a74c9f5a4d5c6bc419347c46f235d8057841848b9ec
a274191a5c77877d8879ffffc109929a752fbf42cdc3a26c4e047846f77ed5a7
ad254429c4ca65874e6ae012c97368604766d18695dadebc843e4fb71a96ba81
42c1ac09526a2efa94342dfaf94ad8e16a09ceeff45bf74cc0ab579700955545

POSSIBLE SECRETS
0d6b8eac96e2087a5e7549625686148f38337a1d78e7b38158c0da4c906baa79
c56c7a5338060719e5bc069d15b58c68034c65cd679c7d65f958d0a872837faf
nCcHhBJ+r5jDr0ERNbOfBIJ/pDQFZIqvHaO2vAiQNRE=
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
a1ca39af40fcb77ed286a4bf11505e9ada570d01bc840f2abb056ecbc97663bf
d0c88b783533c4d13ed089303f6b25403e6709926bef55df315e5d308b2636ff
TdQDsqdcAU8jyTN6NihYJULAUxAJpTfNWWUTPnMXLns=
86f4dbbc4cc096186c7a15db1885cfbc05c558cf9ff1a8e80647beb86508d09c
476d2fe69f6f9d2cc380075dfd9493576a9890d7a63210fc66468c9e957f80a0
5118eccd24640a38140257ed51b74bff21891bb0358051fd759a1fc929337704
46c8b071-5421-4d72-87cb-4b664d7e51b3
119e486acfd625d90ac7b42f3a9e294a075cb8f443d9f471e2ad81aa628ad876
bf763f57c2976fa192f524a0ab016c31b2ae463d47d6a1a57441e9353830a1a0
9cc98ae84ac0d3d48fcfcf43c61c53e3f54203b21e0c96a32405282f2b7341c0
1f9b6f416e03ad562e8f6de51bddd400b9454f3fe58cfb064948c5ec204e38d6

POSSIBLE SECRETS
7ba61c5434ff18117905a89550cfff97464e992df2fbbda326c441ced7b947c2
3qr4mlB52OG3zCTE5HcVTUQ5lTX1MDO7
0d10e13a0da36bd56bbc71548edb97dacdf3808e54eb66f9a8f70e689ca972ca
4c049b1bc6707f0637e0f87205baf5500f904aa995d8da4144938952d6faec1b
7d73d21f1bd82c9e5268b6dcf9fde2cb
b4xBpY1Zr7toyC1sOTTNBO4ImhCct0sLu70B1nFUAHo=
d2491b67aff3cf61e3293f494dfc87996712bef3d300ef4adb7e0a3778d60768
fddc0ceecac286894b8a863ec7fb3c22bbfc01764309832847daee4cc3b72729
de862eec75690e0a1ce1103ffc5c869b3f106085857a512a82e43f7aaa38c523
a0784d7a4716f3feb4f64e7f4b39bf04
b8fa919e202f5341bcd9a059fc9f6673b7f36430a5680f83ef994f87842ecdcd
6c92b2dec1ab2441abc6069d1232a9c74db496c4c003e4d4ac4899749be6d1ba
c946e725f25207abfac017530b8b9c5c3f55e012e768bd605abe063f28c5fd7b
2c5a04751e7a3d9c5da0533f664e2435dad92a311e7e15820e8e659918027120
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

POSSIBLE SECRETS
8a0d6a9ab73c601f179b639ed347b076184e3b16c3cda44bee111e86355c252e
630403a44268323ddbb5c51896a98abbf67a02f1ddfe2e3faff8e5a04675bde6
af60eb711bd85bc1e4d3e0a462e074eea428a8
cf858cda900977be3e4c3c7e11aafe79
708bdc1d6872b4ec0e7e174080786923b3c2e8e596cbba36a2da97678d2709f0
529dd20ad96604f4eb40c3df0cf9e2d269d3ddc1514439d9507a9f55bd6fa908
b04e283a5d9f6597a23c74c815718c3ef88e8b8a3d1b96097b78e3c22a44d2d7
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580801012434427757837678 4
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
2abc6aaa51b4d65294c7d471c3fe2c84258fad29b1057df86b414508f6e79aba
ff4beaa8b09ab169c8943cf16697d94d0dc3445c23be279880e679962fe74445
40e715aef5902c9885b6d4019453f304042d066c93f8a5d7f1b5bc6630b9f16e
bVq06mwryvswJ9TEv8eKHMxwi9DjT7SQH2xL+admUqskqroPQT0vVkasNMzV5jv7
8mLoio5zXFzLNZDTURhMAugjCGrSPBhh3GCaf2t8mPk=
19nlSd1PMyXKl1niHXaxZmvGyLnyitkJHQnkLHtPHLj6n1sor4NdBFlTmnlba7BL

POSSIBLE SECRETS
flTy8eyNabiNCHuPyNX0x482LGXuzWIuGD/71SlN2nKRI9kSJNQ0LUuMwsl06lrx
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
yTyv47DW9aV6rpyU1wL04puCd80cKdCTVtCqLwFmVTX0TBccJdZ4Z0bBqZNN3F0R
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
420c7f73b0c9260a2dc59fca41886b95c4e415c1f961c005b057c5b714f2f1ed
2347444c8107a8d48d715637126025812b9daa36b9394ca4d79edbef57b32dfe
7e8f76580a5a40b4ab16ebd384bd089d4cea53c49a2db53d5ca166a452c4aa39
327ea99ded30e090ceac9a8a3d3b827abc2b4530dc4c08dd82e5f90e9717c78f
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
49e38508e665dd1fd95ebc5a59e0a1777f71bcc0508060e7f7c6df6cbdb9cf30
a2adb603c0b73057d63be62b3557077e07f53f8416b2ba2270acbdf592e00fdd
98d2da587b66873dc281780c81fa6d7030ca1bc5043c7c327c621ae360ae3225
2700a8037654ab729778fec40dc71ae06bc0c6cb92449b32f3a79a8183a25c35
46efcd73d2c1c183b102fb6413c61e0b4f35c6b964f1f60e1cb239d05f50dbf4
1a6b707cb66e0cc7dbebbcf31f0815fd

POSSIBLE SECRETS
e4f3f2519915e6cd2998558858695d1fa24b069d82fc6e9472688d35fa6a0c8b
85b8752fd829e2aea68d9543501c4586f99b6171fc8c07554867ad5c28d17f7b
fcc6770a93b6c709b0d939ec2f2247db9d8157ee564d53a35b9661fc4daf9ba3
55a9b8725747715216a115c674a5b473d1f5d25a8613e0669bbbb00b2482381b
b7a89f974a3f0cc0b8d56347d72e7df5426802054bab87e020705cf55885e846
08f0404102e7d55d5e43c868ab421874
bf1c43d0d6d77e87e10aab6cb54226982619b984c91421f14dc43dc370dbee96
nv6PiabX0G4RLHtriKodA9C0rOBToujvB9ySFMp3wxE=
e9d7a69a61a6506b675e14b22d95a9d37c8bab0bd1a2a7573a66121c2425feb0
241ca2cc9a5ef1631e4e8d493248fffdf50aeb6ff821bfcb66259b36eafdfe4f
0kr13TIqRr0Mkim2K4wTtB+PeWlqdIn0V95/3g6ojAuM6jvjN6OT9QeeEcwm9v6h
c4890ce4ffc97ac070b0abe2c3e96f5e0d065fa6a2b1471765eaf5405a6a1660
pkxrOWj7zD1ScyeXlo8fp1m52MhBIE9QvURtfE4hxB81XVp6EbBK8CYQjvvhYlf1
727e00d9aff3143797d53f9e59297e6a919422bc42f6c930a1590ea82dd7ad56
GajzmnIGCWKypTldGXdzGSwHW6ZZV69Bh6cWfmyAJmA=

POSSIBLE SECRETS
002b196dcf5d865d115ecfec056e93846c7413b8cdab5c7b429cec108184b51f
lVUtMgOC8oCk0OL1R8+dcIzJX9C75UT4Pn6J82++vFrHU4GwQD+682Yf0fGqttpS
9894ef84aa568029bc75225d8d07fc332310de1871534dd15b42e9d3804e90b2
U0xsRAuvio8jauxTatwQyzMnnLPlyOKF
B3EEABB8EE11C2BE770B684D95219ECB
da2-a2e0e734b6eef4d22906cbe792
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a436 16c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f696 43110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333 635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4 d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312 2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d 6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a 92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4d d9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87d d3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148 d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009 0603550406130255533113301106035504081 30a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e6 4726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e6 4726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233 d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e6181 86673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c196 2fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb 21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
50ac8f5e9bd9c4ed8d7d54de9dbd8b7221986b345e25d9fb6ee89b12f6c08778

POSSIBLE SECRETS
1c6a6abcac034ee2eb0a34fbba1b99b2
c1b4bfea2611cde65fca14efcab2d842fa26dab4c8a00524238f1a5333bcc469
e9cce8c2305ddb88e910bfdb86b8c218b81feffce1305805ec401d2996c1d71a
aeaba8bd0f69b864d17a8ff252a71b0d8598adb64d522ab0399399aa27e998e3
3bc1a3628d51d3ec7f663e3ffe8187b6
vDxCHtRyDtZtywG/lqG2i2wEAK0QRlsYMxcEu2Y9QxY=
40c2057893dc0780eea0ce128a41a6518493f38e
c404ca7cd9b38342940bc55b186cbf8ed3b7cad22f9afb6bfcfc18904d7f70f3
bd3d9a76c392c5aecfc9a925826cf326b3fc60739ebbd6926e92bddf42229d30
e772d12a1e4bb5b221d70e3489034b266a7714defa89221f7d3b4da8c68842f1
47c5796e12fc664d69f5a39d3ab0f6d5e35d07ad3a92f23c51270cc70941ae19
32670510020758816978083085130507043184471273380659243275938904335757337482424
798b926b725b0597a7ab4ab998cd94aff4cc536e4cebab8171fc94bd250cfd4c
967a1360c88e18d42cc6c6110a2235ac867074f21b5d9928e0b51f8336fedea4
452f6ea4a3ad660d91bf3fff38e3bd234fed2b9a0f9691bb71787d88a297eabb

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
1b3b9d8625ff30d346282d8a358b72c1f290e589224d17a5ca0656dfdb4d9b5b
85d8c479ba769f468f2930fb7ebc1b18f92c5863cee04bcbf834a7dd35e289ea
fe4ece6e5050eed818cf57f2cfb3514a78dc1567bba4f0185e84d602b493b9be
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
07ce4f50aa97bbc8f0a71d2d4171a1b07441eb9eca27c84e7be4f5e138977711
a96e60624e3e89b6c05711f7d7405ca34e04dac001280a1b49017994727c14ab
2edbcba6f172d2081bd5b16e126de673d4eb857b8640bec37c151b0d564aeb47
d34eeeda5e7f2cd99b4cbcb009fc5175874f34782e030483bfb306f80abc931f
b9a59eba317e0c7f4fc70f6ca27d4e7c74dbba87606123f3c1279f0ccb994a55
GPszzgHpZYiZiAuNUWHrBjQ03NSAuoak
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4b903b3e-59fd-4731-ac4c-da8c29656c0d
13bb137224121ac8c3c4930763feecb52618b30bac1ef788ec3e993412274a16
27cb2817210b92f8ee7fddab786bdbe4c5d0fdd966dcd8a92480cc1ba0cff87b

POSSIBLE SECRETS
9701ff7954fb99965b70d1df3576110359a7a0b2a76bba31981b42332802a881
4f9553c057618ce2e4f6a725c70a87d284e5dec82569c2aae5327a98c1790445
095446bdaf71568e6811abf4e0403ba547a273e47a5e77752a0fa2baa0434b54
91c76dac5d633465096a4bb967b5238ef39a401b1be296f9dc0cea27b987ffbd
11129573b8f456a75942dba5ee7f8396c18c0ef118181e16e9e9820ee49329fd
28ec7b15d6737edbfc23bffb22cec02889b5ddb517a08623da8b6a47e264f635
7Ejn4kVFfkIwTENQCsQUmu0CsZi/nLRRU7QLVgsNDkU=
t30h8UZEoZP8GE77k4AdlDjTvNQpvs7DHs10k6C9ZzU=
Q54q2JslusSv8X8AsH7nKgnoWyF6GsnL4uj/9o5E5cc=
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
f2c12526e66960a637315004cc4b6024ec4d393f178875a004fa4e9f4439a58d
bae8e37fc83441b16034566b
d28461542b470870007e039ee78898457bbbab0e5fa42e4b89338b872955bc89
2a879bf5c8e6db4ed07eff3e2bd5bedf5a0fa0d6fbcd92f8858ce43ecc722715
JFMtS6Z9bzmnMwoeWTxjTTnvJVVZDuewSTBrvx9CdBc=

POSSIBLE SECRETS
116fa884d1ece1aae2c2c757b400a5078b985cc979aad542b8c07c3e99c4cf34
3e7c3c3cdfeab33801a4de945041b05314e7510c8c0fd440a282c5c141676353
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
a25cee21d906be882a026543a2b88e70fd3b4cbb35f521da8afad15d19060cb0
ea2372c464a925ecf9ba3dc493f495406558cb289d0b166ad914d3c5e5ce822e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
9aef61f7cefbf02f26afd58dae2572712a82f7e022712f2688ffdc26b5d186be
484395612939064517590525852527979142027629495260417479958440807170824046352 86
839f03279c64b853e353489e97c1fd9f0812aa4ab73716910cbf83e2a037ad88
39b73791de85bc4bb90840e3ac6907854141ba13dea83d3ce75af7e467f73c17
551795d7cb3d56b027bfd379467544c67e4eeebea24e8edba05154a6cf12f7a3
aa2a6c0085976007fc28d463ce6ba26a4731840d654736863999ac37e1796aad
585860d0a1498c5cc25cb6641b3dc05fe6df7fcd1592e0317dedf66c4d1e8a08
c84d66c8fcd2098d7680ae302ef2ec24cd149e351db188725b0d4977aecb14eb
00e0c30e32be2e72f17c7279e10c5d57548268cca5b5c126c74f3b111eca998a

POSSIBLE SECRETS
315882da95338cf4a27f564d644a348445f7e5d32f0c6af24289e5c6a99ea9c5
de85207d4c837436186d9e3c9bc02bed026e60f8502b69bf71660b4356906819
b632f087716b99b9b3d59a723925fba95d4f340fc6cbad8614839e5fe11cf9f3
fY7ocyET9PuMHUXxIlKP/PpFa5xsSzhwfB8mpep5FSQ=
04b0f3f259798d190ad327dc4a1ecf5e783f3a4bdfd950cacd88593607b83160
9ef38518505241a52ee04e289dffcf6d573e3c19e4cd522ef0a8aedd318a2c62
deca87e736574c5c83c07314051fd93a
dfe75f6f0f0acc41c1dbe87a999ae519593462e0c48dfc04f8d711ad6c18d774
284132d7f447d89d065dc308c11233084f9bf614056777762fcaef543bafac60
fe8824bcbfb080caa961d267dd1aa6fe54c4590e4b49c1977b24093a44fb3931
28faf46144620661e941ae8b35652a9c5dfc2d873ce612ecc23892c4ce972edb
0c3814f3b692698155c16f54aa4d880813b8073e6e0c82ca319560f16f9e79a0
6dfc5351291a144404bf72d3bffc6f5de84c591aedb7feff43ab9ac5ec3999a1
dc87a2447128e5847764f65543053cda16b4a627b160c2a49c3c342cc0861efe
9de78becb67d676298507297a0138c736a1c4c987a38a0257e8c159a39e7d026

POSSIBLE SECRETS
t4LignzpQnyAJJAZeU8P3GGD0dgmuTMT4n9grwU+EMc=
ikPkuPQbpnIYaQGo6Ao4zzPX0Qaf9HhmEZeT4ZfFQOg=
1d21450c89458c9fe97c40066ec0157e99b9592599a708e56fd2e9e84230ab4c
6cb59520de9fa7eee8d275821d5b747686bd9127303a24be600ad4f1f289e49d
MyezUX/G4B4IwyhTDkP3w1lDN+jx4NQ6UyU5K5beVZyubOhn8Q7qD9UAXT+3eaCC
6023b4c7fe33a1a5cfad03b403a5a45e
fd7de40d090a81c69d7dfb02923ca9079eb627daaf0247473cab86ead870e71a
c1eda75b9726a1001bbf9ca2635ed73f
c8e5d4e5f84d195eee829a0526f3e57c513cfff84c41961c76ea541d867fb303
29200FA5-DF79-4C3F-BC0F-E2FF3CE6199A
a228604dfb285ef94a07adc945795909a9eff99067755c0b5058f9fb304385b2
46203620b63ef46334d364ec4658fdd5
5e4fa9b7fc795f22bd40d149048a1534b02c83effb5825c67eb54c1f6eb12b3c
36864200e0eaf5284d884a0e77d31646
785649ff763ed6065cc69f8ee4b43e98a654a1bb86ed77948231fa40fda363c7

POSSIBLE SECRETS
55066263022277343669578718895168534326250603453777594175500187360389116729240
ece2b4dfc1b2f6bb74c51a16585fac83bd45fc8b1e7602f1042910c8edd26ec5
OfZFeGMpPN4nP2QoVlOsW4kmNx194lMXDh8YPc+yAeg=
68ec05965a2036e98353b316a7f2c02c2f8363464bc33f0d38fc310b725df9b9
12f94ba3866d492fc8dd9ebb4ebf8ff0bdbd50f85b95b7b0e7142bee692b2f3a
sha256/V5L96iSCz0XLFgvKi7YVo6M4SIkOP9zSkDjZ0EoU6b8=
8abb1a494ec237f3aad7ea4b7a0c53e95aef62be35476714c25dacdfdcb73d65
1157920892373161954235709850086879078528375642790749043826051631415181614943337
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123319
96986125fa3316985311dbfdc8ac2fb361118ef088b983731f2134d68c656fad
s/IaC73MjD9vpfzZvssIGR7eelXzGompBCRU9Px19GF39ZofYoD29ElcUTZqSvpM
9f613e18df94247bb2f6ffffa6ba5b357468365d7b264d0918edb007ec4a1fac
307237187d95c679378d0977ffe6b0f2304ec6250a0d4d3b144fae49f4f20f55
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733078086511627871
c89db295925f9b3539270587c9675f62eb10da1f62d14ddb7c2871b60f049b26

POSSIBLE SECRETS
3e0ab0fb81779e22ec1da49cbd4e95720a57d1b8b53f0ac60732751adba93dba
e6a7d61c7a5151cb357da8cbcbcf6c1e99d27d8373ab24a1a8f124bb07b88a35
c4da42a3d095997ab2c42e82cb4335d459d645d61ff851d1d91b91ba927fee09
6de229a36d5ab53799beabf241a7158087d085afa139185abeba2b122c1da3bd
cc991c9f1ff40bd1f7fa57f74e3dfec6637d844988d0fa7aed063b605f4bba21
f0abf89ea43b2baf56ff6380d614acf284b821ad1e718660702a781c58b44c46
7c58e91cb2944d42fb1047dce08ea47a6cef195f01e03f117cd66d898f7e017d
2d3937972af7ca6d9d90f11b82c2e6fe
sgSNHgqJ9EwYu8w2dMx3zRGSIiO9D1spUgPO3F51srA=
3ikNbWzMTIqU222KtrzzFiiUcpXtNPU8upxs9wXDAJYxbW4sx23+rx4eBiJjRteZ
7d92b77340f2b4330089701be5e84442e7ac760a96afc54ca36e8e9d20cf76df
c96d3e3bb0f5a3c70db860eeb98e7574e701ebb49685712ad8d0a8f7e267eb49
d17fbed28bf372c3a7bad28f1cb49be6
MvSsZpyfbWT7trIgHlCNNRjqnVxZ1Gq7
017ca571-7b94-48e1-8ffa-61d3f08d09ac

POSSIBLE SECRETS
gWtAtoadyS/0GQFYvFINsjkt4bRjT5fE+w3tC36yAJU=
ad1642e7aa57e2d1e2d925571ce38345e67aa25fd76f9bae024e37ee9191923e
8e8820abe9af84909bf0d67238aac87c68915604a2b73b69d329e5e7cd9208df
dbcea7f0fa5727c3d792e01000664ee65fcc1ec3c6f1528bcf29431c0d99e2f2
fde1378b5d191e22565ad14aca2bc241c48cb78c6b2424fd857d1dc787b56e3c
900c4b3c2a8677a66a3c1d8d423814562ad1efe37a40eeed3858978ef4700599
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
ea1c6b943427809332648ff8ab9ba8156b80d5d968c0f5a8f3f38400cf6c0d15
a6954147ef2e473a54fc8c47f411615034d39f1b92ba8ab99f39cf72686c3ac6
10c752b5f84255a4f7dcd8051ff727d1e96e8bc7e72dd208e5cfd8b9c394dfaa
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
c5ead61db8cf1ae350b1dd24be6806c913ec91ebe628bbe0183cd328e56fc553
96b187bb62f9b8eb86d80909ada4c77595d475f0f881beacac7c212f68814099
dd888060852767cc42b0e38316fe2e690f09cc6c887972666cfbb7edaeca2439
a2c646dab7432263cef774b9752987d98611790326d7c160af779d346baec039

POSSIBLE SECRETS
3Dv+WIEpWKEbBzcuP3SgLUV0aXQTnDSdpPKu/RzIzoY=
08ee566f07de1ca5fb48e795406f7cba6fe754d4b8f93377c2fb3103141bf0a4
EByWffqzraQVS82Db2+ro2d9ZqC8EsuKj9igHJ6rpI4=
3071c8717539de5d5353f4c8cd59a032
e036f00db66a61e8b00c6aae25bbc90e841671505db861269f19fb6fad019440
RRAtLSPp4UfCvUq8TqKgqVcK2MQ98P/X8fWWJOdf6yU=
ba8af87e32166a5bdc8bbe84a114cbc114e0ba396c67e337396a133526269928
36134250956749795798585127919587881956611106672985015071877198253568414405109
707bc51a888363e7fda8eb50510269445d02afa740d8cf29fe914d21b044ccba
c0f40fe308dc96c9c6b1dc66b1db21c878ef98ec525764c5fede1dd145ff243a
849f26e2-2df6-11e4-ab12-14109fdc48df
NnIoFyYmTm9Yd/i5F1TZFAo2tPeZkpFEZBtgPBr60Ow=
dcb428fea25c40e7b99f81ae5981ee6a
830a47df28f4ec78d6e270ff58508414554942a744957f5874daa46e1a6e1ef2
JZBFNEdYFhTFBTCRgtU3dDnkdlKXmKLHUW9VyRRgLZX35JOvzKEIQuHunyCpcG/w

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
a2093098ceab572c44f48ff236df19cad1f6811d6a211074a6b9d8953c8bb687
9625f11561e703ce633897fdee167aaa7d8282669afea68215ff66f446a649cf
21d44a55131c87f6beab4b52e4601b050e96fe3997e2e8216630ec028b3464cd
8cd28c271b03c7d6933de52133221d0550a2bb2d2d8bad1fdd29d8eed37be396
834371d6a1a564b82c602b9e43a80e7445febfab413ce5590e7dd5685c084d0f
5e4671bbf996cc3ba55d8a800b628de3efa2ff1c17aac8d130c673b3005fa584
7c8291a6828127bada489ccbfaf3e1f21bff24da3e9d393729dbeea2c24d2768
4e1b0be3a3811297dedd3be9e144ccc66897c101e235f23592e84b4f89994c2e

POSSIBLE SECRETS
e90c5659e8ea6478422ef148b83c010d496231243a2b9e5a02fe522d8e6455f5
7c96164b182cdb0f4c9433a60dc43a47ef5aad909d42ad5643a33fadbfd9688e
978747a957cb3cd6a01e7c48576b09197b01b1dbda535477be3ec4627c686d43
28cd72c15c5cb237a767ea471f56a8c6d73cfda7ee3ce331475ab046740a64a7
2b352b5da42b52a19df8a90b57778e92844d5d22ea168f9db374b6707240348e

PLAYSTORE INFORMATION

Title: GoodRx: Prescription Coupons

Score: 4.8280053 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.goodrx

Developer Details: GoodRx, 9208596685329031075, None, http://www.goodrx.com, info@goodrx.com,

Release Date: Dec 12, 2012 **Privacy Policy:** Privacy link

Description:

Get the medicine and health care you need with GoodRx. Digital coupons and discounts can be found for prescription drugs, including GLP-1 medications like Ozempic, Mounjaro, Wegovy, Liraglutide, Victoza, and Semaglutide. Virtual care with access to reliable telehealth services and perks when buying prescriptions. Keep track of your medications with your personal drug guide and pill tracker. Save money on your meds with free digital coupons that can help you save more at the pharmacy than Medicare or health insurance. GoodRx is NOT insurance. Pill tracker, meds reminder, and digital coupons - enjoy an Rx app that brings you complete virtual care now. Our free prescription discount finder has everything you need. Virtual health care with a personal medication tracker, rewards on medicine, and custom meds reminder - all with GoodRx. Health insurance benefits like Rx discounts on medicine, senior care, or triage services. Doctors care about our prescription drug savings app that is trusted by millions. Enjoy prescription medication reminders to Rx savings and coupons for a complete mobile healthcare app without health insurance. Get to know your medication list with our drug guide and pill tracker. Price check prescriptions, save money with mobile Rx coupons, & find a doctor for virtual care. Become your own advocate for your healthcare and download GoodRx today to save money on medications! GoodRx Features: Digital Coupons at Over 70,000 Pharmacy Locations - Safeway Pharmacy - Rite Aid Pharmacy - CVS Pharmacy - Walmart Pharmacy - HEB Pharmacy - Walgreens Pharmacy - Target Pharmacy - Vons Pharmacy - Kroger Pharmacy - & more Medication App with Prescriptions Up To 80% Off - Digital coupons let you save more on prescription drugs - Find Rx savings on your medicine when you look up medications - Check Rx pharmacy prices & redeem digital coupons to claim your prescription discount - Medication discount finder to use at local pharmacies

like Safeway, CVS, HEB, or Walmart Pharmacy - Health app with discounted meds & patient assistance programs - Visit your pharmacy or Rx discount location to save on drugs - Save on pet medications too Medication Tracker & Free Pill Reminder - Meds reminder: Make refills easy thanks to alerts with our medication reminder - Medication tracker: Manage medications with our free drug guide and pill tracker Telehealth & My Health Care Tool - Medications list and drug guide for your prescriptions, including GLP-1 medications like Ozempic, Mounjaro, Rybelsus, Victoza, Saxenda, Zepbound, Wegovy, Liraglutide, Tirzepatide, and Victoza - Pill tracker to help with daily prescriptions and medications - Virtual care with online medical professionals - Easily find doctor care without Medicare, Medicaid, or health insurance - Understand your prescription list and medications - Medication delivery & pickup available anywhere to get quick and convenient care now GoodRx Care services include - Refills on birth control medications - Urinary Tract Infection - Erectile Dysfunction - Short term medication refills - Triage services Prescription Discount Finder Trusted by Millions - Digital coupons made easy for everyone - Our medication app shows the Rx pharmacy with savings on drugs, including prescriptions like Ozempic, Tretinoin, and Vyvanse - Healthcare professionals across the country use our coupons app to help patients save money - Featured by: The New York Times, PBS, ABC News, Forbes, CNN, Good Morning America, The LA Times, & more! Upgrade to GoodRx Gold to earn rewards for additional discounts, benefits, and offers. Get exclusive pricing and reliable mobile health care with GoodRx Gold. By downloading GoodRx, you agree to be bound by our Terms Of Use. Read more at http://www.goodrx.com/terms-of-use 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
2025-08-29 23:09:08	Generating Hashes	OK
2025-08-29 23:09:08	Extracting APK	OK
2025-08-29 23:09:08	Unzipping	OK
2025-08-29 23:09:09	Parsing APK with androguard	OK
2025-08-29 23:09:09	Extracting APK features using aapt/aapt2	OK

2025-08-29 23:09:09	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:09:12	Parsing AndroidManifest.xml	OK
2025-08-29 23:09:12	Extracting Manifest Data	OK
2025-08-29 23:09:12	Manifest Analysis Started	OK
2025-08-29 23:09:12	Performing Static Analysis on: GoodRx (com.goodrx)	OK
2025-08-29 23:09:12	Fetching Details from Play Store: com.goodrx	OK
2025-08-29 23:09:13	Checking for Malware Permissions	OK
2025-08-29 23:09:13	Fetching icon path	OK
2025-08-29 23:09:13	Library Binary Analysis Started	OK
2025-08-29 23:09:13	Reading Code Signing Certificate	OK
2025-08-29 23:09:13	Running APKiD 2.1.5	OK

2025-08-29 23:09:21	Detecting Trackers	OK
2025-08-29 23:09:29	Decompiling APK to Java with JADX	OK
2025-08-29 23:10:03	Converting DEX to Smali	OK
2025-08-29 23:10:03	Code Analysis Started on - java_source	OK
2025-08-29 23:10:14	Android SBOM Analysis Completed	OK
2025-08-29 23:10:31	Android SAST Completed	OK
2025-08-29 23:10:31	Android API Analysis Started	OK
2025-08-29 23:10:47	Android API Analysis Completed	OK
2025-08-29 23:10:48	Android Permission Mapping Started	OK
2025-08-29 23:11:03	Android Permission Mapping Completed	OK
2025-08-29 23:11:04	Android Behaviour Analysis Started	OK

2025-08-29 23:11:25	Android Behaviour Analysis Completed	OK
2025-08-29 23:11:25	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:11:37	Email and URL Extraction Completed	OK
2025-08-29 23:11:37	Extracting String data from APK	OK
2025-08-29 23:11:37	Extracting String data from Code	OK
2025-08-29 23:11:37	Extracting String values and entropies from Code	OK
2025-08-29 23:11:45	Performing Malware check on extracted domains	OK
2025-08-29 23:11:52	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.