MOBSF

ANDROID STATIC ANALYSIS REPORT

Reframe (1.0.366)

File Name:	com.glucobit.reframe_366.apk
Package Name:	com.glucobit.reframe
Scan Date:	Aug. 29, 2025, 11:03 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	21	3	3	2

FILE INFORMATION

File Name: com.glucobit.reframe_366.apk
Size: 41.08MB
MD5: 4b4467d0ad0ccd24373bafcd78a5fa5d
SHA1: 3dbe68442f718bdeac06eac4275d8261dd6ac815
SHA256: d856a3bd08f4fee5dd10bc36b19f53729793f7407a86503a8fe7e44cad1f4bac

APP INFORMATION

App Name: Reframe
Package Name: com.glucobit.reframe
Main Activity: com.glucobit.reframe.MainActivity
Target SDK: 35
Min SDK: 26
Max SDK:
Android Version Name: 1.0.366

Android Version Code: 366

APP COMPONENTS

Activities: 53
Services: 15
Receivers: 14
Providers: 9
Exported Activities: 7
Exported Services: 1
Exported Receivers: 3
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=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-05-01 19:07:03+00:00
Valid To: 2053-05-01 19:07:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x32caa29d2a50e3348c7a3250502237a830b0030e
Hash Algorithm: sha256
md5: f528e32d69f4d787bdef0a52d4e7c616
sha1: 86e08e103608ddc42655fcd0d973f98f77cc2643
sha256: f4452f2ab5f25ce206d0aab3cc2ebaca1f1d6051103253e37794235b8977c326
sha512: ce436494dd12c53582a43fa2f4c720de624f66254f123180e4d15c20eb7037fbcf8d38deb4d21921a0af1e274a2d9190131273443f68f71f8da83539dde5cff7
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7e46663e52f1b0b3823eb0a08cb0a716dd4bab76dc139c3a210f1e61eb48b547
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
FOREGROUND_SERVICE_TYPE_MEDIA_PROJECTION	unknown	Unknown permission	Unknown permission from android reference
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.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.
com.glucobit.reframe.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>4b4467d0ad0ccd24373bafcd78a5fa5d.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</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
Build.HARDWARE check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.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.BOARD check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.glucobit.reframe.MainActivity	Schemes: reframeapp://,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.glucobit.reframe,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.glucobit.reframe,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 13 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.glucobit.reframe.ui.screen.dailyTask.ui.dailyActivtiy.activity.DailyWebActivity) 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	Activity (com.glucobit.reframe.ui.screen.dailyTask.ui.coaches.CalendlyWebActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.glucobit.reframe.ui.screen.dailyTask.ui.dailyActivtiy.activity.DailyMotivationActivity) 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
7	Activity (com.glucobit.reframe.ui.screen.dailyTask.ui.dailyActivtiy.activity.DailyJournalActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.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.
9	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.
10	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.
11	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
12	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.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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: 0 | WARNING: 7 | INFO: 2 | 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	Br/a.java Ii/d.java Js/a.java Js/b.java Js/c.java Ks/a.java Lu/j.java Nr/g.java On/b.java com/appsflyer/internal/AFa1uSDK.java fsimpl/C5581ft.java io/agora/rtc2/internal/AudioFocusManager.java io/agora/rtc2/internal/SimpleMediaPlayerSource.java io/agora/rtc2/internal/SurfaceEglRendererHelper.java oc/a.java s2/D.java t2/f.java z2/X.java
				Dq/m.java Dq/w.java F7/C0498a.java F7/C0615eg.java F7/C0918qk.java F7/C0934rc.java F7/C0959sc.java F7/Db.java F7/Gl.java F7/Lj.java F7/Ya.java Hm/C.java Hm/C1847c.java Hm/D.java R/U0.java R5/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Ul/C3048o0.java Ul/C.java Ul/r.java Vm/C3174a.java Z/S1.java b8/C4149H.java c5/C4364L.java c5/C4412l0.java c5/P0.java c5/s1.java cm/C4526f.java com/amplifyframework/auth/AWSTemporaryCredentials.java com/amplifyframework/auth/AuthProvider.java com/amplifyframework/auth/AuthUserAttributeKey.java com/amplifyframework/auth/TOTPSetupDetails.java com/amplifyframework/auth/cognito/AuthEnvironment.java com/amplifyframework/auth/cognito/actions/DeviceSRPCognitoSignInActions.java com/amplifyframework/auth/cognito/actions/MigrateAuthCognitoActions.java com/amplifyframework/auth/cognito/actions/SRPCognitoActions.java com/amplifyframework/auth/cognito/actions/SetupTOTPCognitoActions.java com/amplifyframework/auth/cognito/actions/SignInCustomCognitoActions.java com/amplifyframework/auth/cognito/activities/CustomTabsManagerActivity.java com/amplifyframework/auth/cognito/asf/DeviceDataCollector.java com/amplifyframework/auth/cognito/asf/UserContextDataProvider.java com/amplifyframework/auth/cognito/data/AWSCognitoLegacyCredentialStore.java com/amplifyframework/auth/plugins/core/data/AWSCredentialsInternal.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amplifyframework/core/category/CategoryConfiguration.java com/amplifyframework/statemachine/codegen/data/AWSCredentials.java com/amplifyframework/statemachine/codegen/data/AuthChallenge.java com/amplifyframework/statemachine/codegen/data/CredentialType.java com/amplifyframework/statemachine/codegen/data/DeviceMetadata.java com/amplifyframework/statemachine/codegen/data/OauthConfiguration.java com/amplifyframework/statemachine/codegen/data/SignInData.java com/amplifyframework/statemachine/codegen/data/SignInTOTPSetupData.java com/amplifyframework/statemachine/codegen/data/SignedInData.java com/amplifyframework/statemachine/codegen/data/SignedOutData.java com/amplifyframework/statemachine/codegen/events/CustomSignInEvent.java com/amplifyframework/statemachine/codegen/events/DeviceSRPSignInEvent.java com/amplifyframework/statemachine/codegen/events/SRPEvent.java com/amplifyframework/statemachine/codegen/events/SetupTOTPEvent.java com/amplifyframework/statemachine/codegen/events/SignInEvent.java com/amplifyframework/statemachine/codegen/states/SetupTOTPState.java com/amplifyframework/storage/StorageItem.java com/glucobit/game/twentyFourtyEight/core/ui/CustomColor.java com/glucobit/reframe/data/model/ABTestProperty.java com/glucobit/reframe/data/model/ABTestRule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/glucobit/reframe/data/model/CoachSubscriptionStatus.java com/glucobit/reframe/data/model/DependencyProperty.java com/glucobit/reframe/data/model/ForumProfile.java com/glucobit/reframe/data/model/NativeMeetingToken.java com/glucobit/reframe/data/model/OnboardingScreen.java com/glucobit/reframe/data/model/StripeCheckoutInfo.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java d4/C4826d.java g5/C5647e.java im/C6136i.java io/embrace/android/embracesdk/internal/paylo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ad/UserInfo.java ml/r.java om/h.java om/i.java om/j.java p2/C7204a.java pm/C7357v0.java pm/C7359w0.java pm/C7363y0.java pm/W0.java qm/C7611g.java qm/C7618n.java
				B2/d.java Da/b.java Da/f.java Da/g.java Da/k.java Da/l.java Da/n.java Da/p.java Ea/e.java Ea/h.java Ga/d.java Gu/n.java Ha/A.java Ha/z.java Hu/c.java La/b.java M1/j.java Pb/e.java Qb/f.java Wj/c.java Z1/g.java bb/J.java bb/l1.java com/amplifyframework/logging/JavaLogger.java com/amplifyframework/statemachine/StateMachine$special$$inlined$CoroutineExceptionHandler$1.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/share/LinkGenerator.java com/fullstory/FS.java com/fullstory/instrumentation/Bootstrap.java com/fullstory/instrumentation/init/Initialization.java com/fullstory/instrumentation/webview/WebViewTracker.java com/fullstory/jni/FSNative.java com/fullstory/rust/RustInterface.java com/fullstory/util/Log.java com/miui/referrer/commons/LogUtils.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java d7/C4879f.java d7/C4884k.java eb/C5210a.java fsimpl/AbstractC5483cb.java fsimpl/AbstractC5590i.java fsimpl/AbstractC5592k.java fsimpl/AbstractC5593l.java fsimpl/C5427a.java fsimpl/C5434ag.java fsimpl/C5441an.java fsimpl/C5446as.java fsimpl/C5451ax.java fsimpl/C5453az.java fsimpl/C5457bc.java fsimpl/C5459be.java fsimpl/C5467bm.java fsimpl/C5470bp.java fsimpl/C5481c.java fsimpl/C5485cd.java fsimpl/C5486ce.java fsimpl/C5489ch.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				fsimpl/C5493cl.java fsimpl/C5529dv.java fsimpl/C5530dw.java fsimpl/C5536eb.java fsimpl/C5540ef.java fsimpl/C5557ew.java fsimpl/C5561f.java fsimpl/C5579fr.java fsimpl/C5586fy.java fsimpl/C5594m.java fsimpl/C5599r.java fsimpl/D.java fsimpl/E.java fsimpl/I.java fsimpl/O.java fsimpl/P.java fsimpl/RunnableC5545ek.java fsimpl/T.java fsimpl/V.java fsimpl/aD.java fsimpl/aL.java fsimpl/aM.java fsimpl/aN.java fsimpl/aQ.java fsimpl/aS.java fsimpl/aY.java fsimpl/bI.java fsimpl/bK.java fsimpl/bN.java fsimpl/dC.java fsimpl/dI.java fsimpl/dK.java fsimpl/dS.java fsimpl/dU.java fsimpl/dV.java fsimpl/eB.java fsimpl/eG.java fsimpl/eL.java fsimpl/eO.java fsimpl/eZ.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				fsimpl/fF.java fsimpl/fP.java fsimpl/fQ.java fsstub/b.java hg/C5909a.java k1/AbstractC6334h.java k1/w.java l1/c.java r1/a.java s1/C7812h.java t1/q.java ua/c.java ua/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	Ak/e.java Cc/f.java Gh/d.java J3/b.java Jb/e.java Le/a.java Lu/e.java Nh/b.java Nh/c.java Nh/i.java Nh/l.java Nh/m.java P0/j.java Ql/e.java To/b.java Uf/a.java Uf/d.java Vi/a.java Wr/a.java Wr/b.java Wr/c.java bb/AbstractC4241q0.java bb/C4224i.java bb/D.java bb/l1.java io/agora/utils2/SqliteWrapper.java mf/C6881b.java q3/L.java u0/n.java ua/c.java ua/f.java ua/g.java va/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	H4/d.java Qu/a.java Ru/a.java Sc/d0.java Su/a.java Yu/a.java Zu/a.java hv/h.java j4/C6214i.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	To/b.java fsimpl/C.java xg/C8863b.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fsimpl/C5486ce.java io/agora/utils2/internal/CommonUtility.java io/getstream/chat/android/ui/common/contract/internal/CaptureMediaContract.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	J0/C1984g.java com/amplifyframework/devmenu/DeveloperMenu.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Gc/b.java com/revenuecat/purchases/common/UtilsKt.java fc/q.java fsimpl/aM.java t5/C7990a.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Pb/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Gu/h.java Gu/n.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	Aa/b.java Ak/a.java B2/d.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java fsimpl/C5530dw.java fsimpl/C5564fc.java fsimpl/dU.java fsimpl/dV.java io/agora/utils2/HttpAsyncTask.java io/agora/utils2/NetUtil.java km/C6478r.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	B2/d.java Uf/a.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java fsimpl/C5530dw.java fsimpl/C5564fc.java fsimpl/dU.java fsimpl/dV.java io/agora/utils2/HttpAsyncTask.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	A3/e.java A3/i.java Ah/e.java Ah/j.java Cs/m.java F6/d.java Fg/h.java Fg/m.java Ko/a.java Nu/AbstractC2515b.java Pj/e.java Wj/c.java Wj/e.java Z1/g.java aw/l.java com/appsflyer/internal/AFb1iSDK.java com/revenuecat/purchases/common/FileHelper.java d6/C4871v.java fsimpl/C5486ce.java fsimpl/C5536eb.java fsimpl/dU.java io/agora/mediaplayer/AssetsFileReader.java io/agora/mediaplayer/ContentFileReader.java io/agora/rtc2/internal/gdp/GDPAndroid.java io/agora/utils2/internal/CommonUtility.java jg/C6274a.java oo/C7155c.java q2/e.java q2/w.java xg/C8863b.java y1/AbstractC9045g.java z5/x.java
00121	Create a directory	file command	B2/o.java F6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	io/agora/base/internal/voiceengine/WebRtcAudioManager.java io/agora/base/internal/voiceengine/WebRtcAudioTrack.java
00022	Open a file from given absolute path of the file	file	Ao/C0125u.java Do/e.java F6/d.java Pi/e.java Pj/e.java fsimpl/C5536eb.java fsimpl/C5540ef.java fsimpl/dS.java h6/C5836a.java hs/k.java io/agora/utils2/internal/CommonUtility.java v6/AbstractC8295d.java wi/C8714b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	Bp/b.java Ea/e.java J0/C1983f0.java To/b.java bb/l1.java com/amplifyframework/auth/cognito/helpers/BrowserHelper.java com/amplifyframework/devmenu/DevMenuFileIssueFragment.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java io/agora/utils2/internal/CommonUtility.java ln/C6683m.java mg/c.java mq/C6908a.java q3/C7488a.java q3/C7490c.java q3/G.java
00024	Write file after Base64 decoding	reflection file	v6/AbstractC8295d.java
00012	Read data and put it into a buffer stream	file	Z1/g.java
00191	Get messages in the SMS inbox	sms	Mf/i.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	Ea/e.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java io/agora/utils2/internal/CommonUtility.java m6/a.java q2/w.java q3/C7488a.java
00208	Capture the contents of the device screen	collection screen	io/agora/rtc2/video/VideoCaptureScreen.java
00089	Connect to a URL and receive input stream from the server	command network	B2/d.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java fsimpl/C5530dw.java fsimpl/dU.java fsimpl/dV.java io/agora/utils2/HttpAsyncTask.java io/agora/utils2/NetUtil.java
00094	Connect to a URL and read data from it	command network	fsimpl/C5530dw.java fsimpl/dU.java fsimpl/dV.java
00108	Read the input stream from given URL	network command	bb/H0.java fsimpl/C5530dw.java fsimpl/dU.java fsimpl/dV.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	Ea/e.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java mg/c.java q3/C7488a.java q3/C7490c.java
00009	Put data in cursor to JSON object	file	Ge/c.java Je/c.java d4/r.java xg/C8863b.java
00043	Calculate WiFi signal strength	collection wifi	io/agora/utils2/internal/CommonUtility.java
00034	Query the current data network type	collection network	io/agora/utils2/internal/CommonUtility.java
00130	Get the current WIFI information	wifi collection	io/agora/utils2/internal/CommonUtility.java
00033	Query the IMEI number	collection	io/agora/utils2/internal/CommonUtility.java
00119	Write the IMEI number into a file	collection file telephony command	io/agora/utils2/internal/CommonUtility.java
00083	Query the IMEI number	collection telephony	io/agora/utils2/internal/CommonUtility.java
00014	Read file into a stream and put it into a JSON object	file	F6/d.java fsimpl/C5536eb.java jg/C6274a.java xg/C8863b.java
00005	Get absolute path of file and put it to JSON object	file	F6/d.java fsimpl/C5536eb.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	F6/c.java hg/C5909a.java
00091	Retrieve data from broadcast	collection	X3/b.java ao/C4021d.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java com/stripe/android/link/LinkForegroundActivity.java
00003	Put the compressed bitmap data into JSON object	camera	Ao/F.java d4/r.java
00112	Get the date of the calendar event	collection calendar	fi/g.java
00004	Get filename and put it to JSON object	file collection	Ae/a.java fsimpl/C5536eb.java tg/C8014h.java
00026	Method reflection	reflection	at/z.java ht/C5979j.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java io/agora/mediaplayer/ContentFileReader.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java io/agora/mediaplayer/ContentFileReader.java
00162	Create InetSocketAddress object and connecting to it	socket	Gu/n.java
00163	Create new Socket and connecting to it	socket	Gu/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1bSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1bSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java
00209	Get pixels from the latest rendered image	collection	io/agora/rtc2/video/VideoCaptureCamera2.java
00028	Read file from assets directory	file	q2/C7484b.java
00153	Send binary data over HTTP	http	io/agora/utils2/HttpAsyncTask.java
00030	Connect to the remote server through the given URL	network	Uf/a.java
00025	Monitor the general action to be performed	reflection	io/agora/rtc2/internal/AudioRoutingController.java
00102	Set the phone speaker on	command	io/agora/rtc2/internal/AudioRoutingController.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	Zb/x.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://glucobit-4c326.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/222716385186/namespaces/firebase:fetch?key=AIzaSyDBETmRda5ajZXl-zleBzKx-s2wZZwvUDY. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.READ_CALENDAR, com.google.android.gms.permission.AD_ID, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

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

Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
merchant-ui-api.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
digitalsponsor.io	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
glucobit-4c326.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.stripe.com	ok	**IP:** 52.26.11.205 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
app.joinreframeapp.com	ok	**IP:** 13.52.188.95 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.digitalsponsorapp.com	ok	**IP:** 34.149.87.45 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
monitoring.instabug.com	ok	**IP:** 18.238.109.83 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
errors.stripe.com	ok	**IP:** 198.137.150.41 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
docs.instabug.com	ok	**IP:** 104.16.242.118 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ca.slack-edge.com	ok	**IP:** 18.238.109.34 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
meetings.reframeapp.com	ok	**IP:** 66.33.60.130 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.623768 **Longitude:** -79.559723 **View:** Google Map
sattr.s	ok	No Geolocation information available.
169.254.170.2	ok	**IP:** 169.254.170.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **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
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
reframe-prod.hasura.app	ok	**IP:** 104.18.18.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sars.s	ok	No Geolocation information available.
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
app-measurement.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
amplify-cravingbusterapp-craving-140012-deployment.s3.amazonaws.com	ok	**IP:** 52.217.1.4 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.72.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
reframeapp.io	ok	**IP:** 162.210.195.123 **Country:** United States of America **Region:** District of Columbia **City:** Washington **Latitude:** 38.895111 **Longitude:** -77.036369 **View:** Google Map
docs.stripe.com	ok	**IP:** 54.189.200.54 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
scdn-ssettings.s	ok	No Geolocation information available.
www.theglucobit.com	ok	**IP:** 34.149.87.45 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.tryreframeapp.com	ok	**IP:** 34.149.87.45 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
g.co	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
169.254.169.254	ok	**IP:** 169.254.169.254 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.joinreframeapp.com	ok	**IP:** 34.217.231.110 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 52.21.133.233 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
d2tl7zz537wj2z.cloudfront.net	ok	**IP:** 18.155.174.151 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.53 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.133 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **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
joinreframeapp.com	ok	**IP:** 99.83.190.102 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.reframeapp.com	ok	**IP:** 34.149.87.45 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
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
ns.adobe.com	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
api-paywalls.revenuecat.com	ok	**IP:** 3.226.164.55 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.instabug.com	ok	**IP:** 18.238.109.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
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
sapp.s	ok	No Geolocation information available.
q.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 18.238.109.116 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
docs.amplify.aws	ok	**IP:** 13.224.53.11 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sts.amazonaws.com	ok	**IP:** 54.239.29.25 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 18.238.90.46 **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.
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.revenuecat.com	ok	**IP:** 35.174.220.239 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
email@example.com	Hl/C1841b.java
u0013android@android.com0 u0013android@android.com	Ea/k.java
support@stripe.com	ll/C6629g.java
contactus@instabug.com	e4/RunnableC5093a.java
email@me.co	Jl/C2058a.java
support@stripe.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Mobile Analytics (Amplify)	Analytics	https://reports.exodus-privacy.eu.org/trackers/423
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Instabug	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/206
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

TRACKER	CATEGORIES	URL
fullstory	Analytics	https://reports.exodus-privacy.eu.org/trackers/415

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://glucobit-4c326.firebaseio.com"
"google_api_key" : "AIzaSyDBETmRda5ajZXl-zleBzKx-s2wZZwvUDY"
"google_crash_reporting_api_key" : "AIzaSyDBETmRda5ajZXl-zleBzKx-s2wZZwvUDY"
7973510255192e8d68451edb6661cea72d59de1641bccd5fdbc0b6426bc72a0d
9d2bd312feba652d2ff18fac9d810712f51e150c1dc1c39c56fa176a2edba2ff
74464473-5e28-4244-85e9-2e5fb49bf8c5
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
52e89c50a94a9afc1a07781ff974248b716493119bed7eb63e58a0051fc7a7e0
b5816aad79176a36047f8f79e2184d695c42104bea84ea90306506dce447ac5c

POSSIBLE SECRETS
66a0024710034baa52e8cf46034ae50aa706c0b388760c376eb334ad8339e3ff
b5e9226813f9f3c45d6e4abb60062c036dd5ca6e92f87b60a1f122f7143b5d8e
af5c0412f66286d993a1c971b851ef5f7134531decba56e9c1d7b4457048bbe2
cf3142449fdfe8345f52a6fa3bbd31419244d40e08ba786916d8d9c614afefba
9305fcdaa0006d13fa0ff8d1c857c91dc1b96480d24dfa02dc2a3d3bd6974506
5dc4768fd968953f5b31543bdaaff8bce118fb1e04a57cd41bf13a80fbb97fb1
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
ae70f781-cc71-48a5-8ba8-5f098f359f89
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
069339a0e55baceece1be6da1cce59cb2bba743c01cfd4f3be9869c97098baa1
e3e44c5798b124f6b3d725feaf241d6e01a210ad763c0f510dc8f00fe42acc7a
1a6bada7832c3728281d7783c084f603965f19493b93af32d1ca6e0f78c2a6bb
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f 9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
a634fa34bb388ff1697bd28b6d34f4f8e94b1446121987e04db809c97b7476c2
ba0be68135345ad68afeebc879b87a90bf4e8772ad451ee80290c2f32c4caa05

POSSIBLE SECRETS
eae3e76274792bfa1949de8bbf216cab187181df2ed52befd4e58ce82b4d2b8e
dcffece4e6d7184de5c1ab13fb9a3530a2fd043f851cf4872e1d426bfc43373e
32670510020758816978083085130507043184471273380659243275938904335757337482424
3f6daa5bdb55a2edc57e22e2ff38c6b26c969ccd7ed129fb36ea7d4512ea2257
d484b2319213a4b8fa1562ea1cd8bbd6ab94acceb912c3b4caaa011182672733
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
e3fff20a5a522850e7551b8297e4b8daeb88f211c57f2182e3db6d3534217ae6
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
9d04c0978eb38754bc460b883501392a82c92e4062ebebe89bded200c5f4032e
1bfa26f6e737374e7003b56be72ab8257d97b0b33cf54f5a2807bb3f52c0c9bf
a57a4567c4e95a80e3d95f1d9a61010b17cb10db80d6d7c811c30f233b5b0806
300dc0da4005f38d0bebcfe72ae9d27db2c911e503f68f834fc8253a0dfd680b
55066263022277343669578718895168534326250603453777594175500187360389116729240
b922b1a6d74beea5cf9e82c670cdb4bac2ae960e88a06e560eba554beed524f6

POSSIBLE SECRETS
bf4406cb2434ad1d070e4dc36029b5b8f6de051f5e1d2a5b43c8b701880b5a26
8146c3c386688572a59d9970160400505154cb0bbfb37d030d04e8a74b87a862
5cef1906d45d7e35c9833d50f78a9b6886b9a62863a3350aeed70b19166cb93d
98e80fd73844da9805c03d5d39061576dd9c790ad9976535228bf1fe741b8f11
d4df724e6bb0ffa63769d9f46169897dc302da1ea40b1c6855c1d1c3414015a8
ddc057e1f6cb15bee6ee3ea0f1008d031bb3908ef132d9316c1c8555e9b39fbe
4d00c8a07c08f754787e8d3677657d733f984297701fb1b6b7874da0f487866a
062e3b2bcf975d57d96bd66fbce3a906c8a0caa3efc1c5ca6de20b16f427d6da
1157920892373161954235709850086879078528375642790749043826051631415181614943337
b08c81e80edebb606ad67e814b6739bc335076713dd02847b590d6edd17bd3aa
025c80493a8944ab5f9d91647ab6f06998b3e5e9c77cb2c0dd9a1fba68e9a0a3
9f74b4f51fab87cff3914fe99a6e40464a66f0a3f323514e12d0e1f14e5ad3c4
ab56c549d65d7814721f4e05f1eea9c55aba247db24a623dbb31910cd73d8315
a9fb2b35ba7762ad5fabe931d9eeb1655c9f92884f0d7b354b79a4be875af0c6
1157920892103562487626974469494075735300861434152903141955336313088670978539 51

POSSIBLE SECRETS
86254750241babac4b8d52996a675549
a1a94d6a735bf2fd3af93aa4418306fec898e6965200c0dfbd7e956fc4d1b6ba
11aa8339-8bd4-441c-b1dd-110ad73de916
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
c5862ce5cbf41de3877ed7cd3f8e0868c9ca1e6ae87b71930927ee4ecb4ce40f
59f93124226cf7569b3ee0daac852b840361b5f9b2d7ee0b9ddfe55932fb3c29
0467d08b7f70fbc73414cf578e608ee993647e936020776de6c5d366cf8cbbc1
2502fec0f99b2358be8c08a2e2f7fd4b187ba5485caca9d6f37ad311155ea971
53037e6563414db024f6933ff7ca819f967c5d2e7d40e27c726b8bc6ac0a12f6
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
e1f048189f4ae7090dc480cdd92f1fc8526aea33fdaf0012ba0101076e393a6f
8ba9dac68d7749a2a291118564f25d67114cb31587cc66ac9cc2d0320ac04476
74245fc7a2dfe2fd36ae03df542d63441827024aa81bd1a9573369f90c895f92
0df1e904cba76dce6af4f7c46eb428f356587a3d5c3b94347b7ec87ae8e724e5

POSSIBLE SECRETS
99e645ab9bb055d7719442ad5304642695 18bbae9598edbe08a0e5ed061ea44a
f036b2b6a078b23b16b7e18004c28c1a201122229080a7534247612c3c4e565a
7730e396e60a4c9ad6560e8f28c8bde4220e326211b33f11948e8033fa64dc6e
8296d0bafade012ebeb29bf09cfa4bcffae0e71ea93cf34e687d89d98d21fb44
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
cebcd90485f4845e20081e39917ebc26c7fcb9177455592b9d5d3b104834954e
9ea646222319e905450a77dae340be7cd347274650badaf703d8f8ade24d253c
e49f788b977f86349f009042d129fa2a3847a6a3c537144161e7565c49257a42
3a66b5173ae31b68f45970a3f87a188756e57a20a1194c261ebc647679513097
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
ae86dd57410e7bca5456dd8a3ae900a6b74b8556144a0021ad45274c581310ab
54d81a76c0a2889ccc50a7ad18e6be6ee601daa0c6a5b3c12ffaa1f39d8e3e4e
3107781311999ceaf24b655f06cef04e462e64df5de9bc130581553415ec7f14

POSSIBLE SECRETS
a3b8574e6f37a070cf267ad81c19dd2e95fd026c85a866ad99a3b1ff7e2d226b
2b9d7399e53bc2b2a5b8fed621eb93e27de0440c70a61297dd446d1df0ae4325
9f2482c8878a359f59341fa88e8ef632a8b3a43a1bafec7e3ecae7a28b41e7f5
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
7c47395641c24a7a93af5c63239edfc8417cf3d5d675555c047f9410d45661a8
6146d9a93c99ed91dc1d6a5d30fde00738cbf147088eaa4117cc92d338fbb493
c89ab00883320baf49eb27aa0aa07c90effa50582713a61e6370653294f637c3
fd7e61d1f5cd3d44121fd6d7bb6c3c96201fa1a443771bef1fe1f93765f66bed
80ef122bef243d25c6feb3c5d425e1702369f38e68c9fa62d9b6145752f0a616
484f69c8c6d0b3fff1429842828bc5cf3405827f6ba06b068084b8276de3f68f
n19tirAolyQWBx08BfnnT3BlbkFJdktaWwGKF7Mq8u1RVmvG
515d6767-01b7-49e5-8273-c8d11b0f331d
98481de983da199d9ab17fc36552143a9635077f40726f534535fa65e57dd1a1
51f6c538963b3bd8720be4d1568415fc90fa51746b46d008fd69d782e28fafa8

POSSIBLE SECRETS
d57b2ea5375cc2df591dfe4af2e73644b22a92c2c3354b8d2aa2cc8e4974ede1
b05262b8e619fe9cbf8a6ece434086b135a389ec5561610255c34aed079c7fd1
5e8f300e389a536c0ca68c40fefae7007101127346863791 53afc12cb65d396f
a85a1c09e5aceb0b96610869ad0fdb3210c4b5ab295c4df292cadd332b5c868d
83721c0e3480c37a331c7ad440e6bf4f91221f0e243d1878d39e6af5ad5dfd98
eb4b465c29a41f24a473aa74bc12e61b88a145b2f1155ebd3889867b2a68c35d
4404f4bf4c26102dcded562811eaa8f13bd531d15f7996bdd1a3f43370a369a7
5eQ131xUrPiMZFrBPJA2C6GEzWs0xeZS
d39acfc51fd036a2ebf375ec098d1c5fa766a309b34197b8dbfc860d6945ef50
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
79170d1dcc78ce83f9edecc3b2c8f578d9bb6e33086a97225c028c820bc73677
782f7e511e032e3e4ea4227d34f06e9554fc1a4560c6bf896ad8445d11c57da8
7c1197f68dcc8772e585a73a003919b7adf2025ebfbd389317df178aae02bc30
bd97120dc7a7f24243fcc353dfc171d78866bd8a02e617d47e8965d950a695d8

POSSIBLE SECRETS
f27fab6f96205c14ece06e9f1fd4b969581a7307d577ac3e7acecbf73270938b
2df5ae9ba65a9c2bf7bfae513145e3f6e9c7cc849faefe0075d7721b3245816c
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
5bc571fe78dad9f41a149362eae46b9b682d7ae080c113aaf7dfcf2d1c347116
c678442c4997f9ba03e6011504d2d52a47300a7310849f4c5b4fb88e3196136b
45e7d96330be59a868ce3f31f95d67526f2e3db45ccbd8d68ab83aaf6cba32c3
2d3b27b36aa80085077573a824617dbe3ecac327832ee8cc55d40d87347cbb79
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
29c9520df7138f5f87e6368ec374f9ed3d677ade36f7b475933beebcfe21a06d
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
c911bb76-df21-460a-8fbf-d158beaf3b1f
2077efc1f4d18f97aa77d38725e7b3b514862c1f49446f4679311e18424147b8
823f956e8f9f574534129f7a1924a3ce39b3215643feced93108750653f90805
9b7bf8b3fa166e8a87a7db050b58f7d00cd50e39c79ed4cf98f00738700bdf7c
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

POSSIBLE SECRETS
7126ba210f95e55f0649a3e84d6aba97f1d35223f76d7461a3afac2257c82e2b
308bb0874e519744bd431217fe81551809b909fb795f80d20dd75641b8a43bc2
1046f2a6f7f05223779323d5ccc4116999873ece997d46f3b9921a59b77b4f83
6f9e5d26d8405a2fe771aa3f3c78a112241fabcccace75f06ada2e4eab1cd9a2
e57ea15688634cd2f29ae3a25fd597fc42d22e8ae7eddab849819c401b860e2a
962eddcc369cba8ebb260ee6b6a126d9346e38c5
f6ab76820b508071e031db977625ada7ae3070baf0a3e921416c37ef37eb276c
1d5a03ed5e567a3e60594121e2bf329a405abb6fe2f5155f5c76e9a6232f9e5b
c0fe0af79421f97d15a43b56d45112659cac823f660e6c9f13b118b3044dbe50
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
01a70947a95df69a6de3b94cb939aa00
ecd133a922777f88865bc1717664d0973e15c8fe0f942b0623eb889b70654139
602ffa137f344f1885bccea79d72347a52ec719e94f4cf15dfe95eada3ed9981
1941b7ccdf5db7c8fe2c368748674446b0cc30e840340bac349109f58367cc98

POSSIBLE SECRETS
7d57d152520e4190be87ba2cd2b261134c894e1e9ff1a5970b42a794f9ac83bc
756f294401ecefea42633bdd1cbe4cc11622f5a8a1bd819e233af38baeda7b87
43137e5dedf5da1a2a09f6ede47519f245e570911a1915b087a473d8
79db0bff2c2c8bb67d4033ce345b5db5cca69b22cb46b7bcef928ca358d290fe
0d154d1acea85e3c977c6a9d08924e784ee3079ace6f8b33c077ae2849708094
5f813139b61b550a7f225abbe0e4c9e1eedbf29e3c8597707bb8b0d73448a50a
388d7fca622a59ad335c95c61324b3294d72e0b980f2d89a6fffa33eb435b0ba
f28f8ce297e1d48f6507a4bdd9fa2b6e1aa80b06c343d8e58ff449ab5c438703
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
b7916b4fa7d775c9edd4e16627aa95f41b5e13bc13cf861cab947e70f7b86b0a
c0c996c7a83e53aae95c8cbf4c5eb3c7c8adc6d3219f470b096e7346e742c643
a443bea9a75bb21c16e8e67678e7b99cf3255304073e15b8acb3614ef6ca4af6
1a9b8a73f321b2334a855d7154006c36ed1bb1e9167a55ec71a29255af146b9e
845248aef19a578b1130a31c2b42d927be9729b7a00d3fe685ae2cfc8d14226d
b2d515e24c09a721f5d72ead814f7dfac784c12e9606f64e33fd8693bcef6817

POSSIBLE SECRETS
e37ec9082e023c78bd50cfe80cb5a1cd9fdf1e68079b446693eb202e8ba6765f
1c8b7e4e74745e2bfd87624137521d5ab4e04a16dbde5d37a3c08c2d0f6d842f
1ae06c017fec1fdef565709a0c366a7df45456e3b6ad614d22118a9fde40407b
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
a03a6a2bee966b0bddcba2d0fffd2424b3fd83d511fea0921b334c13ae725cc9
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
12a693e59a499fefa666231d5d676fa3267f4ad27a39ef9cc3945f35f4ca6abb
d557ea52-400a-463e-a555-63b75b159713
15cc7cbc-7561-459d-a13b-e34ca7f154b6
df112b9513e8abdf7844f02ba5714ba9484a6104e43fed1ee4a333d80aff9e5d
9330d3cb84d3ce0d06b9fee91d875edfabbd903f63fa04d0573c50ee93a5810f
dc684c0477086c4bbf540af7ef30a96ac3c7ed221aec5ddf775d93cb63f69e88
3bfb0b3b1d382b4a0791d669595573a3c814d4d3bee1d14cc0dabd7f9bab1fa6
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

POSSIBLE SECRETS
3b5ee176de1f3f099514ac6e8759ff52dff1d177cffeda1aeb46682e5e4e670d
dd441af20dc51a8ffd2348ec0cd2815d98142c87604192ee426a93f23059157e
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3e488855e46e29e4abc9783dac654dc3b8467862803a6f61bef640d1f2f8a3c9
9992d2490725d0cdd91c5ce3a328900c333feb9ed9e8d2b17adc1881892e8a5e
25cc42c0688ea0497edf82f5e93e6ed13cff7d54bb5bd01fc7343e6f16645002
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
58dbf016ca31430e9ed66a451a8a800cfc06670cb754ec3ae8b1b6fff0c8a586
f7a0bd65dd173ed7078da91a3395f90a322de524f228374f866201632d4d91e1
542db555019b88cca92d52d84bbf57f3d3691e59161faeed73840f132d63844b
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
6b37b14256c19128cde41ac66634b9513520359d47705150b9331315d7e9bd3c
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a

POSSIBLE SECRETS
602a9126d16bbc5ddfdf124f2101c646e0425de65d8b53757423453719d575eb
73bb190bfd85c90ac14bbf067d6eb566
f883915c396b42ccee072b8bd1e1d20624641349f221a51af6d3c407cc3b4d22
b5741880afe532810605a6950d7f430f9f529a4a8881433860462f0732624eec
a65517b1e6df52e7191ad60f618c1b51f7f513512d3f753dcb7be6c5ade085ea
484395612939064517590525852527979142027629495260417479958440807170824046352 86
7d92c8874ea7fda899505c35e3b6baf3fd02a9736c4ed5c6ef2e9af3769de5b0
dc54254dc67478b7a412b823da0e653c24d86db4d64940439546840b8d23f211
5266aa41754d1c2e32728b90e947ab54105ee224b7ecec703793582d2c1ec774
42645393743b2c012449a995ba811dfe0ba603861a14824cd99334f5f3c17fcd
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311 2316
39a4988bc60846410a099dbffaee241675da518eb1d31348244b4ddd320c7804
1d19381d2785b9c117b57e5ed388221e9288ae09aad8a1d0ff8513d6a257565e
139afdd2ecc569cdc18a730bd727e99ba2cbfebe593edd5e9018410c7a6186e4
95a2e7eae2a907bdf29853db95e2cff4c6288c97e2bdbd3a567b5a6b61f5425a

POSSIBLE SECRETS
8fcb1079-3923-4437-adea-0b1fb726031a
8941140b60f72983098c98dc6b5a7ed189e8fb72c975972032577bbdf0fc280c
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
f7221add6864f955a6724367ee5c2182884567f914725d2ae3370f1b5106072b
c878d241883c7d9c8e435bc142a8720f7a3c2fcbd34ef1f499770af4a499c129
962e759cc23dcf52355faf238f858d405d9f23985bba39016a9c91e0f75d812f
51IWubdD12Dp8zl9wequGIf9rZeaIFsPlvfSc7D1N1wCQhluAlQcWCfTdrbFEEsMojRbJTP9FCu48lErH9vhggHLT00BjkMjEXU
0e4ff8f5f94e9ffc2bd97554e2c942f10aeb6dfa6978d137742a92de04ccae58
9760508f15230bccb292b982a2eb840bf0581cf5
aa5b19c897c8415a2d1f8d58215fc7643d2e3cacf9d198ab6eee9d0cce421506
6207fc9f40fbfef41cb9675f7a996264f2736e9ec56c7529cc8b231f275a11a1
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
7c35e4e03227d44e4322fc5f9e669f345b94af9f7389933134e7e342ed5f5292
2f6b143b9922a2db300b9a278d9d9e5190c61eae1ca607599d6b758de6d9608a
3613425095674979579858512791958788195661110667298501507187719825356841440510 9

POSSIBLE SECRETS
dc99b6152513fa3fc6b232adc4d56fb8d848a9363c211b5903a43a1be0d912d2
9f6b24bbba67e5718525193d5114bfc26f6f14230b978759b10560358a0df056
8bc70ffe53031d9b2f642feac9a479d603ecbca194cc24c78b38d6a8d3f6ce3b
9b2ea672fdcad373103474adf10fcac4b33b525d2ab1b179f56f996b6ce08f86
55d7b0537a50427be1074a716446028c8748bfdaae93d16ba2a9c34f22e4a397
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
bb433ae46676b89ef1f3508c9cdc4e0a32ebc798f9a62f9fa523696961725f4f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
3d3364539dcba88dc9d145ee6271e2a24ecf2d5bd306b51a3bd8d9c0955aeacd
3392ef3f555d985a7e8ef31fa56a56c292546d41a770a08225ab7a215d21ef77
05d0c32f80b5afa59b2d7540227e39ddfdb986dd6fc738657c4876b49ac17b66
d2288a7de71f8d3696e19161571ad37e921de9fd4b56cfa051d9786a9dab6113
9e025154481f24850a087e5b0fa232df5ae1af2f0395d6e6414b888dbb62092d
a2cbbde8d7a3091903bf1999ce70ffaec65c9d911a27f8819b0e563344c09aa9
6f280891c0e8f47e58e63d19be46fdb71564cf4695be0497f3f94cd727a2a27e

POSSIBLE SECRETS
16c82cc0bdb60f25f1dd8f7e4bb380cf17956a33f5fe5e20a043783b121cd9d6
f1be652e-b710-4e95-8252-6169bfdcba1b
5775c697dd75fee836857a92e69c68d9e5b5918f18922bf93b5700567a89bc1c
dcb428fea25c40e7b99f81ae5981ee6a
e340600d58f2587146d3447a3f3b18df81cbbd9c348084c9c16497c2e805a3b0
d6dbbfe963ea7a29c3ccdc97a6ab1daf8f84eca9989298c2a5eb394f77b7c7ac
74a2903a16ae8c795deb3f0148421dc36bfdc2709b69d9f41886beadc78ac53a
8c094de696417c4c2efe8b3955a39f526aef1c06c79725cbd78a5179d715abf2
eb103a920cf6b50a29b183df303d0c53215ea1c747a88bf252c89a06b4523787
f98776324bcdced5564d3857185c99ff73402181e43f996037ed8b9366cabf5c
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
4a90b0280b71cdc4f4daf4102ef98120ecf7cd7333f11f13ed88966cdf510a3d
deca87e736574c5c83c07314051fd93a
d03defd44a0f5e7f0aac40356d9b703c26ee3c3a131e3bbff2ab98d35373081e

POSSIBLE SECRETS
69c7070a08a296f53243b215ea617ccd25d490f180dfa926c7eb761ce5c3ebcc
1bdba8847e6851bf193e93e84e3b9d6cf0fca4bd03f423a78714fff7da51004d
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
aa8130e0-66fc-11e0-bad0-0002a5d5c51b
2581d9f423b414975781942ce224c2b4df832ed5ccf9f6f10f285337f44633b7
81e70d1da8ee8ab1556f4673461a4d8be6047e2511da1b5b2cd5395b4aefe487
c9253fddd2241a6a858d9a72aa8ea74702217d67269210ddf72dc1a2b6604cf6
04b4bb907e250913b916a29849e061f4c5a04072450f0d0a4198b8d7c30e354f
8d5155894229d5e689ee01e6018a237e2cae64cd
4122af49589a21173928f35248f5513064fab7e2a3ffebead9407f6284fa945d
503e6177a8c4dce62dffb7c96e73fcf83f823a4cdf2e09d7d9933b6effe171e8
c797ea16be82c5dab359891559f852403a48ae59a388fbc12570c436488b8b5d
dd2592c9cc146acaaeb4277b7169e4f02e4e601831ae661810414783b2a5e3eb
f7043b4c5e65c7b73d10ad800d2418065573603d8783b2cdaa69929f955e3ba0
6ada58dadedd66f180863f4d1f7630cd4178198669fd13a8894c02aef242c780

POSSIBLE SECRETS
e5c78429-b68d-44a2-8a49-834bba0032be
970632382789c0348ace7983dbc7d622cc888d8516ee40045f9da587294a1255
644a0eaa347c46100c1db14b24059798b4f97c4e524088f59a56da90ec43a33a
5ca505f15d73cf47f78c37e16cf6c2d80768920df85a2120550d5541c869b9df
3dbd54d32e6be20faabbdb1a738f31e2fc7cdf6747acc4754a4e9a3152005e83
ecf46da08c203e561dc062b4c156fd294f8d08153492d9fdf0b89387a60672bc
c96c6fd61927a00bf52f4fbae6ef0633c76cc6c20b148fbaf069ff82187260c5
b1119ec6373a2642a2b6988b727b941eb76bef214d29f37e4ff3af3ed199c5ea
66f685631c1bd7f0ede1d18058a06de0d0728b8c179d4e3c46601b9efe14e83b
f7461fa98c8b8678b2aa4cbee4d3d708d46a4e0deea014b610c989b837247b13
51IWubdD12Dp8zl9wc8aZiXsqBqxOxv0KmfEWBz4z6tIxwTo0pCDbSbp6FG6DMCbTpyiJDUagZaYFsaAaOeM5XN0t00qo6YT3KY
3c1c434859d1400878bf9a3c0f57dddfeeb54829979c6fd37778551ca2d9a8fc
fa0923891c07dd69656b0c5767033a31d0018f5d06b910a289e1d8371650084d
840e640c5cf05d2b50300704bbe796a5779ad47dd3abe5eea2e043dbde4deae9
e468b7f799494b72b5413587973ed54b04730ba51672ffd17d833af9169be0c1

POSSIBLE SECRETS
7a46b841df8864069d42826084a9a5c73d3ecd2b46f6b3fb3d94ecb36e98f4ef
a4dbb7eb1b4c10daf7cd021ffe6c2ff518716bc1add3258ea272bb7e1daa4f18
bf87ce71b9b2fe566081b41f7282c62da426344f1b29570152f8e76207d679c0
49ddc88955b819374554ca89e47deea4e936eed7aba1ac3443bd2a7630d8fbeb
1cbd3130fa23b59692c061c594c16cc0
933fb05dab56f989cd3f2ee3662c2c823d1b8ce9196283e058c504e1505eac80
b184ebb857cf102aeef359e60e443a7e68c8edc8e94e55b5cc1485ab49e494ae
385920537e67b871ad3595e2b181b6d13cd13c664dd39dc9af6ca024708552d1
f1b300b194f2e811ec024c9e608d8bda90814daee06d04c932ad9a1592bebccd
3482195b635cabad51e9d4e70fe7e2f8bfcdbfd1b9b0987be92042d1d8a4b01b
a46bc0c7fd60a73c85f2bc85a6538952ccf613ae366297e04e9eba8ae705cb81
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
769ea58d6d92b715585675eec79f902bb1f7dc53ea582e33f1eefb2aefedf816
f1f5e000-c151-41f3-bf03-d719148bec94
33098aa4b5652a6f8fbbebb6fef4ffc4ecb225b42d9a82b3654fdc797db2c558

POSSIBLE SECRETS
516fdb590d6dd48eec7317189696c944d80450bf9aeba27ab0ed924798d5a3d8

PLAYSTORE INFORMATION

Title: Reframe: Cut Back on Alcohol

Score: 4.7108436 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.glucobit.reframe

Developer Details: Glucobit Inc., Glucobit+Inc., None, https://www.joinreframeapp.com/, support@reframeapp.com,

Release Date: May 25, 2023 **Privacy Policy:** Privacy link

Description:

Manage and change your drinking habits so that you can drink less and live more, thanks to the #1 alcohol reduction app. Here at Reframe, we do science, not stigma. Is your goal to take control of your habits, cut back on drinking, or to quit addiction? Reframe is your go-to sobriety tool and drinking coach. With a neuroscience-based approach, daily tasks, and live meetings, you'll stay accountable and track your progress. Experience the full power of our sobriety program that gives you access to a 7-day free trial to help you quit now. 91% of Reframe users report that in just 3 months, they were able to see a difference in drinking habits, significantly cut back. With a core 160-day, evidence-based education program, progress tracking, a private community, and a multitude of tools (think meditations, games, and more!), you've got everything you need to reshape your habits at the click of a button. As a personal drinking coach, the program helps you build sustainable changes, develop healthier habits, and stay on track as you detox. Substance abuse will take over your life. If you're ready to make a change, trust Reframe to help you cut back on drinking or to fully detox. Find support and resources every step of the way, whether you're looking to cut back or seeking a sobriety coach to help you quit addiction. APP FEATURES: QUIT ADDICTION NOW OR CHANGE YOUR DRINKING HABITS WITH OUR SOBRIETY COACHES - Find a support system within our private community that helps stop substance abuse - Stay accountable with daily check-ins from your drinking coach FREE ALCOHOL TRACKER - Cut back, reshape your habits, or quit now - Our unique program is tailored to you and your habit-change goals, or to entirely stop alcohol abuse RESEARCH-BACKED TOOLS FOR HABIT MANAGEMENT - Find sobriety or better drinking habits with mindful meditation- try it out with our 7- day free trials - Reframe courses help you change your drinking patterns and build lasting habits with a free alcohol tracker - Quit addictions and learn to beat cravings at the touch of a button when you reach out to your drinking coach through a free sober app Need extra support? Uplevel your alcohol-free or alcohol-reduction journey with Reframe's premium Thrive Coaching and get 1:1 access to a certified recovery coach, personalized strategies for managing change, exclusive video content, and live coaching calls. Reframe the way you think and drink with a 7 day free trial. . APP SUBSCRIPTION AND PRICING TERMS Reframe currently offers auto-renewing subscriptions for accessing the app. Payment will be charged to Google Play Store Account at confirmation of purchase. Your account will be charged for renewal 24-hours prior to the end of the current payment period. Prices listed in the app are USD and may differ outside of the United States, depending on country of residence. You may turn off auto-renew at any time by accessing your Google Play Store account settings. Payment must be canceled at least 24 hours prior to renewal. To read Reframe's terms of use & privacy policy, please visit: https://www.theglucobit.com/terms-of-use and https://www.theglucobit.com/privacy For more information or feedback, please contact us at support@reframeapp.com.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 18:41:45	Generating Hashes	OK
2025-08-30 18:41:45	Extracting APK	OK
2025-08-30 18:41:45	Unzipping	OK
2025-08-30 18:41:46	Parsing APK with androguard	OK
2025-08-30 18:41:46	Extracting APK features using aapt/aapt2	OK
2025-08-30 18:41:46	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 18:41:46	Parsing AndroidManifest.xml	OK
2025-08-30 18:41:46	Extracting Manifest Data	OK
2025-08-30 18:41:46	Manifest Analysis Started	OK

2025-08-30 18:41:46	Performing Static Analysis on: Reframe (com.glucobit.reframe)	OK
2025-08-30 18:41:47	Fetching Details from Play Store: com.glucobit.reframe	OK
2025-08-30 18:41:47	Checking for Malware Permissions	OK
2025-08-30 18:41:47	Fetching icon path	OK
2025-08-30 18:41:47	Library Binary Analysis Started	OK
2025-08-30 18:41:48	Reading Code Signing Certificate	OK
2025-08-30 18:41:48	Running APKiD 2.1.5	OK
2025-08-30 18:41:53	Detecting Trackers	OK
2025-08-30 18:41:57	Decompiling APK to Java with JADX	OK

2025-08-30 19:04:01	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/4b4467d0ad0ccd24373bafcd78a5fa5d/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/4b4467d0ad0ccd24373bafcd78a5fa5d/4b4467d0ad0ccd24373bafcd78a5fa5d.apk'], 999.9999845996499)
2025-08-30 19:04:01	Converting DEX to Smali	OK
2025-08-30 19:04:01	Code Analysis Started on - java_source	OK
2025-08-30 19:04:10	Android SBOM Analysis Completed	OK
2025-08-30 19:04:31	Android SAST Completed	OK
2025-08-30 19:04:31	Android API Analysis Started	OK
2025-08-30 19:04:51	Android API Analysis Completed	OK
2025-08-30 19:04:51	Android Permission Mapping Started	OK
2025-08-30 19:05:20	Android Permission Mapping Completed	OK
2025-08-30 19:05:21	Android Behaviour Analysis Started	OK

2025-08-30 19:05:51	Android Behaviour Analysis Completed	OK
2025-08-30 19:05:51	Extracting Emails and URLs from Source Code	OK
2025-08-30 19:06:02	Email and URL Extraction Completed	OK
2025-08-30 19:06:02	Extracting String data from APK	OK
2025-08-30 19:06:02	Extracting String data from Code	OK
2025-08-30 19:06:02	Extracting String values and entropies from Code	OK
2025-08-30 19:06:08	Performing Malware check on extracted domains	OK
2025-08-30 19:06:16	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.