ANDROID STATIC ANALYSIS REPORT

Kardia (5.44.1-3c4c0ce0b4)

File Name:	com.alivecor.aliveecg_762.apk
Package Name:	com.alivecor.aliveecg
Scan Date:	Aug. 29, 2025, 7:21 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
5	58	4	3	1

FILE INFORMATION

File Name: com.alivecor.aliveecg_762.apk
Size: 100.27MB
MD5: 7195c34f7a05cdccbf99fe88e03dcb52
SHA1: 2fc75351a0bd61d2585b7f2e169d8b9108cd1a66
SHA256: bf0e30f89bfffeac3064d3f56009f1b100e00a2db9e5eee7b271b17591656155

APP INFORMATION

App Name: Kardia
Package Name: com.alivecor.aliveecg
Main Activity: com.alivecor.aliveecg.SplashActivity
Target SDK: 35
Min SDK: 26
Max SDK:
Android Version Name: 5.44.1-3c4c0ce0b4

Android Version Code: 762

APP COMPONENTS

Activities: 149
Services: 21
Receivers: 20
Providers: 5
Exported Activities: 30
Exported Services: 4
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=AU, ST=QLD, L=Ashmore, O=AliveCor Inc, OU=AliveCor, CN=www.alivecor.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-03-21 06:41:07+00:00
Valid To: 3012-07-22 06:41:07+00:00
Issuer: C=AU, ST=QLD, L=Ashmore, O=AliveCor Inc, OU=AliveCor, CN=www.alivecor.com
Serial Number: 0x241094e7
Hash Algorithm: sha256
md5: 33ffb032d12f7766740259929b675303
sha1: 883cf06eef76826ad4345cb733e049db0efde412
sha256: 40ca7e6054892560ba9f3b8573e08d5e7de895abb4f253e2261712ca8a8b3315
sha512: 8d87fa3d68a75ce6b1a059e368f4b139ebf27d6511c4a9b21bcf56f8e84ab1ab795c06ba6a8b1c601816d6df1a94fe0d4e527cc4254fc654a48c750888355dcc
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7ef57317633cc333fe5f66755d67ea7bb6854aed82694a74e7971ce92e7ee7a7
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.BODY_SENSORS	dangerous	grants access to body sensors, such as heart rate.	Allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.alivecor.aliveecg.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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_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.
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.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.alivecor.aliveecg.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>7195c34f7a05cdccbf99fe88e03dcb52.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>emulator file check
possible VM check</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></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.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.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
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name 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>

<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>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM 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
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
network operator name check
subscriber ID check
emulator file check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.alivecor.aliveecg.SplashActivity	Schemes: aliveecg://, kardia://, https://, http://, Hosts: m.alivecor.com, www.kardia.com, Paths: /,
com.alivecor.aliveecg.ScreenCreateRecordingExternal	Schemes: kardia://, Hosts: m.alivecor.com, Paths: /create_recording,
com.braintreepayments.api.DropInActivity	Schemes: com.alivecor.aliveecg.braintree://,
com.braintreepayments.api.BraintreeDeepLinkActivity	Schemes: com.alivecor.aliveecg.braintree.deeplinkhandler://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **46** | 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.alivecor.aliveecg.kardiav2.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.alivecor.aliveecg.kardiav2.ui.profile.AboutActivity) 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
5	Activity (com.alivecor.aliveecg.kardiav2.ui.learnmore.TourActivity) 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.alivecor.aliveecg.kardiav2.ui.learnmore.InnerCircleLearnMoreActivity) 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.alivecor.aliveecg.kardiav2.ui.learnmore.CarePlanLearnMoreActivity) 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.alivecor.sync.AliveAccountAuthenticatorActivity) 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.alivecor.aliveecg.ScreenCreateRecordingExternal) 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	TaskAffinity is set for activity (com.alivecor.onboarding.SetupWelcomeActivity)	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.
11	TaskAffinity is set for activity (com.alivecor.onboarding.TriangleSetupActivity)	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
12	TaskAffinity is set for activity (com.alivecor.onboarding.TriangleManualActivity)	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.
13	TaskAffinity is set for activity (com.alivecor.onboarding.Triangle6LeadManualActivity)	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.
14	Activity (com.alivecor.ecg.record.ConsumerEkgActivity) 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	Broadcast Receiver (com.alivecor.aliveecg.notification.LocalReminderReceiver) 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.
16	Broadcast Receiver (com.alivecor.aliveecg.ReregisterAlarmReceiver) 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.
17	Broadcast Receiver (com.alivecor.aliveecg.SelfUpdatedReceiver) 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.
18	Activity (com.alivecor.ecg.record.AliveCorDefaultActivity) 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
19	Activity (com.alivecor.ecg.record.determination.DeterminationActivity) 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.
20	Activity (com.alivecor.ecg.record.determination.DeterminationDetailsActivity) 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.
21	Activity (com.alivecor.kiwi.publicrecordapicommon.ui.onboarding.SetupPairingActivity) 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.
22	Activity (com.alivecor.kiwi.publicrecordapicommon.ui.record.ekg.EKGRecordActivity) 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.
23	Service (jp.co.omron.healthcare.communicationlibrary.ohq.OHQNotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
24	Broadcast Receiver (com.alivecor.telekardia.utils.TCAlarmReceiver) 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
25	Activity (com.alivecor.telekardia.TKAppointmentValidationActivity) 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.
26	Activity (com.alivecor.telekardia.TKPushNotificationManagerActivity) 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.
27	Activity (com.alivecor.telekardia.TKRescheduleAppointmentActivity) 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.
28	Activity (com.alivecor.telekardia.ui.payment.retry.RetryPaymentActivity) 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.
29	Activity (com.alivecor.telekardia.AppointmentIntakeFormActivity) 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.
30	Activity (com.alivecor.telekardia.TKWaitingRoomActivity) 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.
31	Activity (com.alivecor.telekardia.TKViewAppointmentDetailsActivity) 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.
32	Activity (com.alivecor.telekardia.TKCollectFeedbackActivity) 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
33	Activity (com.alivecor.telekardia.TKBookAppointmentActivity) 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.
34	Activity (com.alivecor.telekardia.ui.download.PreviewDownloadReportActivity) 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.
35	Activity (com.alivecor.telecommunication.audio.TCAudioCallActivity) 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.
36	Activity (com.alivecor.telecommunication.chat.TCChatActivity) 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.
37	Activity (com.alivecor.telecommunication.video.TCVideoCallActivity) 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.
38	Service (com.alivecor.telecommunication.service.ConsultationNotificationKillService) is not Protected. [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.
39	Activity (com.braintreepayments.api.DropInActivity) 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.
40	Activity (com.braintreepayments.api.BraintreeDeepLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
41	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.
42	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.
43	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
44	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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
45	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.
46	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.
47	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: **5** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	F0/Preference.java com/alivecor/data/models/DrugIngredient.java com/alivecor/data/models/SyncChangeRecord.java com/alivecor/pro/r.java com/braintreepayments/api/VisaCheckoutConfiguration.java com/opentok/android/DefaultAudioDevice.java io/grpc/internal/R0.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java x3/C4927g.java z3/C5062d.java z3/p.java z3/x.java
				A/d.java A3/i.java A3/j.java Aa/c.java B3/e.java B3/i.java Ba/c.java Bc/a.java C3/a.java Ca/a.java Cc/b.java D/t.java D3/c.java D3/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				D3/g.java D3/t.java D3/u.java D3/v.java D5/k.java Dc/c.java Dc/e.java Ea/a.java F3/h.java Fa/a.java Fa/b.java G/c.java G3/C.java G3/C0999c.java G3/C1002f.java G3/F.java G3/n.java G3/p.java G3/q.java G3/u.java G5/a.java G6/o.java J0/a.java K/c.java K3/a.java K3/d.java K3/j.java K6/h.java L4/f.java L7/a.java M0/c.java M1/e.java M3/d.java M9/d.java N8/e.java N8/f.java N8/i.java O1/t.java O3/i.java Oc/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				P3/i.java T3/a.java T4/d.java T7/c.java W/c.java X6/a.java Y/a.java a7/d.java b0/C1639a.java b7/C1677b.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/alivecor/ai/H.java com/alivecor/aliveecg/P4.java com/alivecor/aliveecg/kardiav2/MainActivityViewModel.java com/alivecor/aliveecg/kardiav2/model/diary/MedicationDiaryItem.java com/alivecor/aliveecg/kardiav2/ui/profile/C1955n.java com/alivecor/aliveecg/kardiav2/viewholder/history/ekg/HistoryPremiumViewModel.java com/alivecor/api/RecordServerApi.java com/alivecor/common/ui/AcKitAnimationView.java com/alivecor/data/models/DrugLog.java com/alivecor/ecg/record/AbstractC2432v3.java com/alivecor/ecg/tagsandnotes/TagsViewModel.java com/alivecor/neuralsuite/NeuralSuite.java com/alivecor/rest/c.java com/alivecor/telecommunication/audio/TCAudioCallActivity.java com/alivecor/telecommunication/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/alivecor/telecommunication/video/TVideoCallActivity.java com/alivecor/universal_monitor/audio/AudioInput.java com/alivecor/universal_monitor/bluetooth/BluetoothDeviceController.java com/alivecor/universal_monitor/devices/BLEDevice.java com/braintreepayments/api/C2575l0.java com/braintreepayments/api/C2597p2.java com/braintreepayments/api/R3.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/cardinalcommerce/a/R0.java com/cardinalcommerce/a/S0.java com/cardinalcommerce/a/x1.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/a.java com/github/mikephil/charting/charts/b.java com/ibm/icu/impl/C.java com/ibm/icu/impl/C2874w.java com/ibm/icu/impl/G.java com/ibm/icu/impl/J.java com/ibm/icu/impl/Q.java com/ibm/icu/impl/Y.java com/ibm/icu/impl/w0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ibm/icu/text/T.java com/ibm/icu/text/V.java com/nexmo/minirtcsdk/MRTCMediaNative.java com/nexmo/minirtcsdk/MiniRTCNativeLibrary.java com/nexmo/minirtcsdk/devicelayer/AudioFocusListener.java com/nexmo/minirtcsdk/devicelayer/DeviceLayer.java com/nexmo/minirtcsdk/devicelayer/DeviceLayerPermissionManager.java com/nexmo/minirtcsdk/devicelayer/NetworkReceiver.java com/nexmo/minirtcsdk/devicelayer/OnNetworkConnectionStateChangedListener.java com/opentok/android/BaseVideoCapturer.java com/opentok/android/OtLog.java com/wdullaer/materialdatetimepicker/date/h.java com/wdullaer/materialdatetimepicker/time/RadialPickerLayout.java com/wdullaer/materialdatetimepicker/time/c.java com/wdullaer/materialdatetimepicker/time/d.java d0/C2948a.java d7/g.java fd/b.java gd/a.java gd/c.java h0/C3188b.java hd/a.java i7/C3311i.java j/MenuItemC3406c.java l2/G3.java l2/L4.java l3/C3843B.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				l3/E0.java m0/[illegible].java m3/v.java m6/l.java n1/C4113t.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java o0/s.java o0/z.java o2/C4258a.java o3/C4260b.java org/joda/time/tz/DateTimeZoneBuilder.java p/d.java p8/C4360a.java pub/devrel/easypermissions/AppSettingsDialog.java q0/C4385a.java q2/C4393b.java q5/AbstractC4399a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r7/C4459a.java r7/C4460b.java r7/C4461c.java s/f.java t0/C4602d.java u/C4679a.java u0/C4683a.java v3/C4762a.java w0/C4801b.java w3/d.java w3/e.java w5/C4820a.java w8/C4850a.java x0/C4884M.java x5/m.java y2/m0.java y3/c.java y3/e.java z3/C5067i.java z3/RunnableC5066h.java z3/k.java z3/q.java z3/z.java z5/i.java
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	l2/a.java K5/M.java K5/W.java S7/g.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/database/SQLiteDatabase.java t0/C4601c.java
4	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	E2/r.java o3/C4260b.java o4/C4266a.java w8/C4850a.java y4/C4995a.java yc/C5032A.java yc/M.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	Ec/s.java G9/i.java L9/f.java L9/h.java Rc/d.java Rc/h.java Wa/a.java Wa/b.java Xa/a.java io/grpc/internal/B0.java io/grpc/internal/C3395t0.java io/grpc/internal/E.java io/grpc/internal/G.java jp/co/omron/healthcare/communicationlibrary/ohq/a.java la/C3912c.java la/e.java m6/L.java
6	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	B4/c.java com/alivecor/api/HmacKeyConfigManager.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Ac/i.java L2/o.java Nc/c.java Nc/d.java Nc/i.java Nc/j.java com/alivecor/rest/e.java com/braintreepayments/api/C2583m3.java f8/C3135a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	B8/b.java com/airbnb/lottie/network/NetworkCache.java com/alivecor/data/models/BpDatabaseItem.java com/alivecor/sync/C2494a.java l3/E0.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	c4/C1707a.java yc/C5032A.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	O1/k.java com/alivecor/api/util/DeviceRootValidator.java com/cardinalcommerce/a/s1.java i7/w.java yc/C5032A.java
11	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	com/alivecor/telekardia/utils/f.java n2/C4129b.java o0/z.java o4/C4266a.java y2/C4968b0.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	b4/C1658b.java
13	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/alivecor/telekardia/utils/f.java n2/C4129b.java net/sqlcipher/database/SupportHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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/alivecor/aliveecg/kardiav2/ui/care/purchase/PlanSelectionWebViewFragment.java com/alivecor/fcm/InAppMessagingWebViewActivity.java
15	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/alivecor/aliveecg/kardiav2/ui/care/purchase/PlanSelectionWebViewFragment.java com/alivecor/fcm/InAppMessagingWebViewActivity.java
16	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	E8/p.java
17	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/alivecor/aliveecg/UserProfile.java
18	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/alivecor/sync/C2494a.java
19	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	J0/c.java
20	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	yc/u.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	D/t.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	D/t.java
00112	Get the date of the calendar event	collection calendar	com/alivecor/aliveecg/UserProfileActivity.java com/alivecor/telekardia/ui/timeslot/TimeSlotSelectionFragment.java jp/co/omron/healthcare/communicationlibrary/ogsc/i.java l3/E0.java w8/b.java
00192	Get messages in the SMS inbox	sms	com/alivecor/aliveecg/presenter/bp/H.java com/alivecor/aliveecg/presenter/weight/j.java l3/E0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	H1/e.java M9/d.java Q0/T.java com/alivecor/aliveecg/KardiaConnectCodeActivity.java com/alivecor/aliveecg/V1.java com/alivecor/aliveecg/deeplink/a.java com/alivecor/aliveecg/kardiav2/ui/determination/a.java com/alivecor/aliveecg/kardiav2/ui/profile/ManageRemindersActivity.java com/alivecor/aliveecg/presenter/bp/H.java com/alivecor/aliveecg/presenter/bp/ManageBpDevicesActivity.java com/alivecor/aliveecg/presenter/onboard/OnboardActivity.java com/alivecor/aliveecg/presenter/weight/j.java com/alivecor/ecg/record/AbstractC2432v3.java com/alivecor/ecg/record/S6.java com/alivecor/kiwi/publicrecordapicommon/ui/onboarding/LocationPermissionDeniedFragment.java com/alivecor/onboarding/SetupLocationPermissionDeniedFragment.java com/alivecor/sync/AliveAccountActivity.java com/alivecor/sync/DialogVersionCheckerActivity.java com/alivecor/telekardia/utils/k.java com/braintreepayments/api/C2565j0.java l3/E0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	H1/e.java com/alivecor/aliveecg/V1.java com/alivecor/aliveecg/deeplink/a.java com/alivecor/aliveecg/kardiav2/ui/profile/ManageRemindersActivity.java com/alivecor/aliveecg/presenter/bp/H.java com/alivecor/aliveecg/presenter/bp/ManageBpDevicesActivity.java com/alivecor/aliveecg/presenter/weight/j.java com/alivecor/ecg/record/S6.java com/alivecor/telekardia/utils/k.java com/braintreepayments/api/C2565j0.java l3/E0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	E2/r.java O/m.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/alivecor/ai/G.java com/alivecor/ai/z.java com/alivecor/aliveecg/sharing/SavePdfService.java com/alivecor/telekardia/utils/f.java g2/b.java l3/E0.java n2/C4129b.java n3/C4133d.java o0/z.java o2/C4258a.java o3/C4260b.java o3/C4262d.java o3/C4264f.java o4/C4271f.java s4/c.java t0/C4602d.java y2/C4968b0.java y4/C4995a.java yc/z.java z8/C5080a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	C8/c.java D3/g.java F6/g.java O/m.java Pa/l.java Pa/n.java R0/b.java U1/a.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/alivecor/aliveecg/sharing/PrintActivity.java com/alivecor/pro/C2489s.java com/bumptech/glide/load/a.java com/cardinalcommerce/a/R0.java com/ibm/icu/impl/C2874w.java e5/C3045d.java l3/E0.java m4/b.java n3/C4133d.java o0/z.java okio/Okio__JvmOkioKt.java org/joda/time/tz/ZoneInfoProvider.java pa/C4374a.java pa/C4375b.java q0/C4386b.java u8/C4710b.java v3/C4762a.java
00012	Read data and put it into a buffer stream	file	U1/a.java com/alivecor/pro/C2489s.java n3/C4133d.java
00191	Get messages in the SMS inbox	sms	com/alivecor/sync/C2514v.java l3/E0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/alivecor/aliveecg/AbstractC1825d.java com/alivecor/aliveecg/EcgReviewActivity.java com/alivecor/aliveecg/EkgHistoryActivity.java com/alivecor/aliveecg/KardiaConnectCodeActivity.java com/alivecor/aliveecg/MedicalConditionActivity.java com/alivecor/aliveecg/TagSearchCreateActivity.java com/alivecor/aliveecg/TagsAndNoteActivity.java com/alivecor/aliveecg/UserProfileActivity.java com/alivecor/aliveecg/kardiav2/MainActivity.java com/alivecor/aliveecg/kardiav2/ui/bp/OmronBpDevicePairingActivity.java com/alivecor/aliveecg/kardiav2/ui/care/innercircle/InnerCircleFragment.java com/alivecor/aliveecg/kardiav2/ui/care/upsell/UpSellActivity.java com/alivecor/aliveecg/kardiav2/ui/diary/DiaryFragment.java com/alivecor/aliveecg/kardiav2/ui/profile/C1935d.java com/alivecor/aliveecg/kardiav2/ui/profile/C1956n0.java com/alivecor/aliveecg/kardiav2/ui/profile/HealthDetailsActivity.java com/alivecor/aliveecg/kardiav2/ui/profile/ProfileFragment.java com/alivecor/ecg/record/ConsumerEkgActivity.java com/alivecor/fcm/FCMService.java com/alivecor/overread/AnalysisReportActivity.java jp/co/omron/healthcare/communicationlibrary/ohq/e.java
00054	Install other APKs from file	reflection	com/alivecor/aliveecg/T2.java
00025	Monitor the general action to be performed	reflection	com/alivecor/aliveecg/KardiaConnectCodeActivity.java com/alivecor/aliveecg/T2.java
00125	Check if the given file path exist	file	com/alivecor/aliveecg/T2.java com/alivecor/aliveecg/stethio/ui/StethIODetailsFragment.java com/alivecor/overread/AnalysisReportActivity.java e1/U.java l3/E0.java y2/C4968b0.java z8/C5080a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	M9/d.java com/alivecor/ecg/record/S6.java com/alivecor/telekardia/utils/k.java l3/E0.java yc/C5032A.java
00026	Method reflection	reflection	ob/C4293a.java ob/C4294b.java
00049	Query the phone number from SMS sender	sms collection	jp/co/omron/healthcare/communicationlibrary/ohq/e.java
00065	Get the country code of the SIM card provider	collection	com/alivecor/aliveecg/AppPreferencesActivity.java com/cardinalcommerce/a/u1.java
00132	Query The ISO country code	telephony collection	G6/J.java com/alivecor/aliveecg/AppPreferencesActivity.java com/cardinalcommerce/a/u1.java l3/E0.java
00009	Put data in cursor to JSON object	file	S7/g.java com/alivecor/aliveecg/P0.java com/alivecor/sync/C2518z.java l3/M.java y2/C4968b0.java yc/C5032A.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	yc/C5032A.java

RULE ID	BEHAVIOUR	LABEL	FILES
00130	Get the current WIFI information	wifi collection	com/cardinalcommerce/a/RunnableC2653b1.java yc/C5032A.java yc/M.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	yc/C5032A.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java com/alivecor/sync/C2518z.java y2/C4968b0.java yc/C5032A.java yc/M.java
00076	Get the current WiFi information and put it into JSON	collection wifi	yc/C5032A.java yc/M.java
00082	Get the current WiFi MAC address	collection wifi	yc/C5032A.java
00162	Create InetSocketAddress object and connecting to it	socket	Nc/b.java Nc/j.java
00163	Create new Socket and connecting to it	socket	Nc/b.java Nc/j.java
00056	Modify voice volume	control	org/otwebrtc/voiceengine/WebRtcAudioTrack.java org/otwebrtc/voiceengine61/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java
00183	Get current camera parameters and change the setting.	camera	com/opentok/android/DefaultVideoCapturer.java org/otwebrtc/Camera1Session.java org/webrtc/Camera1Session.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	S7/n.java com/cardinalcommerce/a/u1.java
00034	Query the current data network type	collection network	com/cardinalcommerce/a/u1.java
00089	Connect to a URL and receive input stream from the server	command network	Ea/a.java F6/r.java T7/b.java com/bumptech/glide/load/data/j.java n3/h.java
00030	Connect to the remote server through the given URL	network	Ea/a.java F6/r.java com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/j.java linc/com/amplituda/FileManager.java
00109	Connect to a URL and get the response code	network command	Ea/a.java F6/r.java T7/b.java com/bumptech/glide/load/data/j.java n3/h.java
00189	Get the content of a SMS message	sms	B4/f.java o0/C4230d.java
00188	Get the address of a SMS message	sms	B4/f.java o0/C4230d.java
00200	Query data from the contact list	collection contact	B4/f.java o0/C4230d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	o0/C4230d.java
00201	Query data from the call log	collection calllog	B4/f.java o0/C4230d.java
00096	Connect to a URL and set request method	command network	Ea/a.java F6/r.java T7/b.java com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java linc/com/amplituda/FileManager.java n3/h.java
00153	Send binary data over HTTP	http	n3/h.java
00024	Write file after Base64 decoding	reflection file	E2/r.java com/airbnb/lottie/LottieCompositionFactory.java
00094	Connect to a URL and read data from it	command network	F6/r.java T7/b.java linc/com/amplituda/FileManager.java
00108	Read the input stream from given URL	network command	F6/r.java T7/b.java com/braintreepayments/api/C2633x.java
00208	Capture the contents of the device screen	collection screen	org/otwebrtc/ScreenCapturerAndroid.java org/webrtc/ScreenCapturerAndroid.java
00042	Query WiFi BSSID and scan results	collection wifi	yc/M.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	yc/M.java
00139	Get the current WiFi id	collection wifi	com/cardinalcommerce/a/RunnableC2653b1.java yc/M.java
00115	Get last known location of the device	collection location	yc/M.java
00066	Query the ICCID number	collection	yc/M.java
00135	Get the current WiFi id and put it into JSON.	wifi collection	yc/M.java
00067	Query the IMSI number	collection	yc/M.java
00113	Get location and put it into JSON	collection location	yc/M.java
00016	Get location info of the device and put it to JSON object	location collection	yc/M.java
00123	Save the response to JSON after connecting to the remote server	network command	Ea/a.java
00079	Hide the current app's icon	evasion	G0/q.java
00147	Get the time of current location	collection location	l3/E0.java
00121	Create a directory	file command	com/alivecor/aliveecg/stethio/ui/StethIODetailsFragment.java l3/E0.java y2/C4968b0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	F6/c.java l3/E0.java
00071	Write the ISO country code of the current network operator into a file	collection command network file	l3/E0.java
00104	Check if the given path is directory	file	l3/E0.java
00128	Query user account information	collection account	com/alivecor/sync/AliveAccountActivity.java
00033	Query the IMEI number	collection	J0/c.java
00199	Stop recording and release recording resources	record	org/webrtc/CameraCapturer.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java y2/C4968b0.java yc/z.java
00014	Read file into a stream and put it into a JSON object	file	pa/C4375b.java
00114	Create a secure socket connection to the proxy address	network command	Jc/f.java
00102	Set the phone speaker on	command	com/opentok/android/DefaultAudioDevice.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/alivecor/telekardia/ui/upcoming/ViewUpcomingAppointmentDetailsFragment.java y3/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	com/alivecor/telekardia/utils/e.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://aliveecg-android.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/242230815243/namespaces/firebase:fetch?key=AIzaSyBo5xFkcu0gh53x1gXgPSze37P_lGUKBDQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.GET_ACCOUNTS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.CAMERA, android.permission.READ_PHONE_STATE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	11/44	android.permission.AUTHENTICATE_ACCOUNTS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, android.permission.ACTIVITY_RECOGNITION, android.permission.READ_CALENDAR, android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.MODIFY_AUDIO_SETTINGS

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

DOMAIN	STATUS	GEOLOCATION
www.mayoclinichealthsystem.org	ok	**IP:** 23.204.250.85 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.content.image	ok	No Geolocation information available.
www.kardia.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
dev-alivecor-us.myshopify.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
www.protocol.netdoc	ok	No Geolocation information available.
www.protocol.doc	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
c.paypal.com	ok	**IP:** 151.101.193.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
centinelapistag.cardinalcommerce.com	ok	**IP:** 198.217.251.251 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.609699 **Longitude:** -122.386948 **View:** Google Map
bugreport.java.com□java□□□□□□□□□□bug□□□□□□□□□□□□□	ok	No Geolocation information available.
www.protocol.verbatim	ok	No Geolocation information available.
alivecor.zendesk.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
www.protocol.https	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
s.firebaseapp.com	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bugs.java.com	ok	**IP:** 23.213.190.84 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.654209 **Longitude:** -79.567108 **View:** Google Map
eu.alivecor.com	ok	**IP:** 3.72.151.180 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
global-kardia-production.alivecor.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
omronhealthcare.com	ok	**IP:** 104.20.28.93 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.sandbox.braintreegateway.com	ok	**IP:** 159.242.242.129 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **View:** Google Map
us-telekardia-production.alivecor.com	ok	**IP:** 54.161.81.179 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
api.braintreegateway.com	ok	**IP:** 52.40.66.148 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.paypal.com	ok	**IP:** 151.101.1.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
eu-kardia-api-dev.alivecor.com	ok	No Geolocation information available.
us-telekardia-staging.alivecor.com	ok	**IP:** 98.82.143.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
centinelapi.cardinalcommerce.com	ok	**IP:** 198.217.251.250 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.609699 **Longitude:** -122.386948 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
c.sandbox.paypal.com	ok	**IP:** 151.101.3.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.mayoclinic.org	ok	**IP:** 23.204.250.85 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.content.audio	ok	No Geolocation information available.
us-kardia-production.alivecor.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ws.nexmo.com	ok	**IP:** 168.100.81.10 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
eu-alivecor-staging.alivecor.com	ok	**IP:** 18.199.108.95 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.cdc.gov	ok	**IP:** 23.52.208.211 **Country:** Argentina **Region:** Ciudad Autonoma de Buenos Aires **City:** Buenos Aires **Latitude:** -34.613152 **Longitude:** -58.377232 **View:** Google Map
www.protocol.ftp	ok	No Geolocation information available.
bugreport.java.com	ok	**IP:** 23.213.190.84 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.654209 **Longitude:** -79.567108 **View:** Google Map
www.alivecor.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.protocol.mailto	ok	No Geolocation information available.
b.stats.paypal.com	ok	**IP:** 34.106.92.18 **Country:** United States of America **Region:** Utah **City:** Salt Lake City **Latitude:** 40.760780 **Longitude:** -111.891052 **View:** Google Map
us-kardia-staging.alivecor.com	ok	**IP:** 98.83.230.1 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.protocol.systemresource	ok	No Geolocation information available.
www.protocol.http	ok	No Geolocation information available.
eu-kardia-k8s.development.alivecor.net	ok	No Geolocation information available.
www.zetetic.net	ok	**IP:** 18.238.96.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
store.kardia.com	ok	**IP:** 54.161.81.179 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.protocol.jar	ok	No Geolocation information available.
www.heart.org	ok	**IP:** 104.18.26.158 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
global-kardia-staging.alivecor.com	ok	**IP:** 98.83.230.1 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.nexmo.com	ok	**IP:** 168.100.80.10 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stagingapi.stethio.com	ok	**IP:** 18.211.107.33 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
bugs.java.com□□□□□□□□□□□□□□	ok	No Geolocation information available.
www.protocol.file	ok	No Geolocation information available.
us-kardia-api-dev.alivecor.com	ok	No Geolocation information available.
www.http	ok	No Geolocation information available.
eu-alivecor-dev.alivecor.com	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
alivecor.myshopify.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
eu-kardia-staging.alivecor.com	ok	**IP:** 18.194.30.141 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
eu-kardia-production.alivecor.com	ok	**IP:** 3.72.151.180 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
support.apple.com	ok	**IP:** 23.40.173.114 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
api.stethio.com	ok	**IP:** 52.5.2.146 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.opentok.com	ok	**IP:** 168.100.107.249 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
alivecor.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cmsdk.cardinalcommerce.com	ok	**IP:** 198.217.251.250 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.609699 **Longitude:** -122.386948 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aliveecg-android.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
braintreepayments.com	ok	**IP:** 151.101.67.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.protocol.gopher	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.paypal.com	ok	**IP:** 151.101.65.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.paypalobjects.com	ok	**IP:** 104.18.34.93 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.251.15.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
us-kardia-k8s.development.alivecor.net	ok	No Geolocation information available.
www.content.text	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
connectivitylibrary@omron.com	z8/C5080a.java
sales@alivecor.com	com/alivecor/api/ApiKeyException.java
support@alivecor.com support@alivecor.com□	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "c14d8ed8b478449fb448a989b275d21f"
"content_authority" : "com.alivecor.aliveecg.ecgcontentprovider"
"firebase_database_url" : "https://aliveecg-android.firebaseio.com"
"google_api_key" : "AIzaSyBo5xFkcu0gh53x1gXgPSze37P_lGUKBDQ"
"google_crash_reporting_api_key" : "AIzaSyBo5xFkcu0gh53x1gXgPSze37P_lGUKBDQ"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"password" : "Password"
"user" : "User"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"choose_user" : "□□□□□□□"
"could_not_authenticate_account" : "□□□□□□□□□□□□□□□□"
"enter_password" : "□□□□□□□□"
"enter_your_password" : "□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"mdtp_deleted_key" : "%1$s□□□□□□□"
"reset_password" : "□□□□□□□□□□"
"select_user" : "□□□□□□□"
"user" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Tilgangsnøkkel"
"user" : "Bruker"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passwort"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"user" : "Benutzer"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wachtwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Toegangssleutel"
"user" : "Gebruiker"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□"

POSSIBLE SECRETS
"guest_user_name" : "%s(□□□)"
"user" : "□□□"
"user" : "Utilisateur"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"user" : "Usuario"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"user" : "Utente"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"choose_user" : "□□□□"
"could_not_authenticate_account" : "□□□□□□"
"enter_password" : "□□□□"
"enter_your_password" : "□□□□□□□"
"guest_user_name" : "%s□□□□"

POSSIBLE SECRETS
"key_code_entry_banner_title" : "□□□Kardiacare"
"reset_password" : "□□□□"
"select_user" : "□□□□"
"user" : "□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"choose_user" : "□□□□□"
"could_not_authenticate_account" : "□□□□□□"
"enter_password" : "□□□□"
"enter_your_password" : "□□□□□"
"reset_password" : "□□□□"
"select_user" : "□□□□□"
"user" : "□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasenya"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Adgangskode"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Adgangsnøgle"
"user" : "Bruger"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "گذرواژه"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "گذرکلید"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "პაროლი"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■-■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wagwoord"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Wagwoordsleutel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Парола"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"choose_user" : "■■■■■■■■■■■"
"could_not_authenticate_account" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"enter_password" : "■■■■■■■■■■■■"
"enter_your_password" : "■■■■■■■■■■■■■■■■■■■■■■"
"reset_password" : "■■■■■■■■■■■■■■"
"select_user" : "■■■■■■■■■■■"
"user" : "■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Salasana"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Avainkoodi"
"user" : "Käyttäjä"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Лозинка"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasinal"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Hasło"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Klucz"
"user" : "Użytkownik"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Geslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Sandi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "ລະຫັດຜ່ານ"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "ກະແຈຜ່ານ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parolă"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Fjalëkalimi"
"user" : "المستخدم"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Zaporka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Лозинка"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Şifre"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Aðgangsorð"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Aðgangslykill"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parool"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Pääsuvõti"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Slaptažodis"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Pasahitza"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Sarbide-gakoa"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Jelszó"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Azonosítókulcs"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"user" : "Пользователь"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Iphasiwedi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parole"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lösenord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Nyckel"
"user" : "Användare"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "סיסמה"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Nenosiri"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Գաղտնաբառ"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Անցաբառ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Сырсөз"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■□■□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■□□■■■■□■□■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Kod"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"user" : "User"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"user" : "Usuário"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Palavra-passe"
"user" : "Utilizador"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"user" : "Felhasználó:"
"user" : "Uživatel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

POSSIBLE SECRETS
E91CB1A3-4F83-4449-B9D2-01021BF20645
CE8759BF-F7EF-4131-A850-032CCD29BEBD
41058363725152142129326129780047268409114441015993725554835256314039467401291
b305b680-aee7-11e1-a730-0002a5d5c51b
45FA26B9-0BD1-4612-A9D5-CA54DFAF534B
2F99D8B6-8ABA-426D-8465-75FA21D076E7
CA78DD94-0A98-46B4-BAFC-C3918469591C
ba903733cb17ed050a41e5bf344e09dd
49123040-aee8-11e1-a74d-0002a5d5c51b
CBE9F2F3-75D3-4FEA-B337-DF7EB82D19BB
8A7840B5-C2E0-438E-A9A1-F601BA50ED9A
5E20FADB-D90A-433B-9BC9-5D23A63217AF
999EFF53-2D15-4A25-B465-039F727C89AA
26584d407930d52f3d62ef77e729f1b4
10e1ba60-aee8-11e1-89e5-0002a5d5c51b

POSSIBLE SECRETS
61D3F8BD-2172-4272-957E-60F586B7EE3D
91D602E4-C183-40B0-BEF5-DC13ACA22489
8D03709F-499B-4938-92FE-4785411DCB24
3DE7926A-179F-47FC-A4AA-F74F14A1EA88
10e2f82a4283346b0d7dcb281d8634bf
D3D760C2-769E-4BEB-85A3-5CD1D4FE0E59
AF1D552B-2956-4322-8A98-23F472358962
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
0782C828-153D-4872-BEDF-742B84BB6584
35EA2B25-B3B0-4213-B1F1-8B5A4DC7CA5B
BCA228A4-364E-4AC1-A246-555772568B88
B077B74E-73AF-45C3-873E-530CC12EB5B7
115792089210356248762697446949407573529996955224135760342422259061068512044369
0FD227A4-F006-410E-B0BB-E5D6F3BCC667
4B481056-E25A-41B9-943C-84AF06D62AB2

POSSIBLE SECRETS
0C427465-7495-4911-ACEB-D7E96A7FF45C
138546B8-A63A-4319-8AEA-56D2CE9CCD0D
CEF9189F-1472-4D4B-9F61-F2CC1B5B11AE
F446A97D-7400-4CF4-9368-5CD55E9B7F8E
CA5C7D57-2C21-4187-A9A1-FF092A3835C3
FE19A93F-16B9-4D3F-A1EC-8C1B3A742E30
D247FA25-8894-4470-914C-781F13B7E20F
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
9639AD63-43D0-4472-AB2D-022B32300919
2E19D2E7-B2AE-4710-A5F6-E95AE342B9DC
FF312DBF-9F1A-44D4-AD4B-2E455C738B6F
B3B79803-9DC9-4802-B6C4-28AB7E677BA4
D8C726CA-E480-4479-AA86-69EAA3F89439
49249A1D-8518-42C2-811E-35767BE1B037

POSSIBLE SECRETS
5926E5FA-8FF9-4E99-8651-7C5A947D6219
2A5FC37D-FD50-4A69-8F0C-26C55E682787
27D5FDAB-45BA-4988-8D8D-DD22EE54E572
23699102-aaf1-4834-858f-4f789db77a0d
A71BCE3A-7563-4409-8D9D-8F2430E7777D
E9E79029-0B9E-44E0-9690-0C7F428934FC
2C7F87D9-95FC-49F1-B047-77035A68C7D2
36E477E6-EBBE-4C1C-9FBB-65C5EBE1590F
FCCB4C55-7D85-4048-9453-C491E9B774F3
55DA417D-22EC-499C-A136-60B7D8BB7744
aee957f2-0d93-4bc2-abcb-a9363b5f40f5
7A1F24F1-B88D-4EDE-93C6-5B0783261AC8
0975B853-CB77-4289-AF06-5A9B0CE7BC48
7244C63E-13EE-462C-80EC-5D6D46B4739F
9CFCF809-3EEC-4417-84C2-B35F4E2A87AD

POSSIBLE SECRETS
0601C7C6-FB53-43DF-944D-AD76A1FB9D09
6e4000f3-b5a3-f393-efa9-e50e24dcca9e
25551BA1-B96D-4857-BC90-4392CD917A1A
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
AC010002-328C-A28F-9846-5A8AA212661B
d5cf2e00b9281147bb926bf4333d63a3
85641B39-8234-4C96-97AE-984FF13F9319
2C04BA9A-1836-41CE-B119-157870A5505B
fd9e2474-0145-41eb-b685-79f18509c7ab
EBFDAC7F-FE8F-43DD-A53D-B6B87935E1EA
06E553F1-0FB0-4187-AEE1-14E988F30397
5128ce60-aee8-11e1-b84b-0002a5d5c51b
7E3B47FB-F305-4DB3-B83F-4172CA667C81
9A1AA6A1-4CFB-4AFD-B599-26DE70CE9289
x34mMawEUcCG8l95riWCOK+kAJYejVmdt44l6tzcyUc=

POSSIBLE SECRETS
AC010003-328C-A28F-9846-5A8AA212661B
9E2F131B-8EA4-4582-AE29-FDA38A26F796
DE471168-DC78-44FB-85FC-91367EC35338
47C52318-8D07-4509-9E17-F4E4F2052193
2AE3490E-E81E-40D1-A5C5-C21ACB1D8F5E
694C8478-77F0-49E0-A04B-E2E10F1704A4
AC4D9774-4BEC-4D1B-ABA0-24944C278437
C6E0DC92-01E3-4AB2-8275-108E4B9F6849
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1
61F892D2-E4B4-4AFC-AE9D-A7FEDBCEDDE0
BD783466-BBBB-4996-AADA-989711317EC0
CA7F3FFF-553B-4190-A188-6B658EE4A485
B5EC10AB-DF13-4168-96FE-C35E55859036
A42BF790-F77D-45EB-B4EA-62CC8C298FC8
17513B19-41B4-4A8D-80B6-81147FD371B3

POSSIBLE SECRETS
B17D9545-B575-405C-B11D-FD396809F5F0
51DFC54A-0F99-4FF0-8AEA-71F5987FFF06
A3D0DD55-D229-4928-AC0B-D97505981E4A
EF598DD4-1834-46A5-BDA2-0A0506A8E8EA
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
9FA7E2E0-EC4A-4D77-BD7C-6F9543962566
5A339FCC-CD2E-451F-9BD4-751BBB9D11E6
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
E4140C92-7CBC-4C36-ABD0-39EDEC0327D8
55D34851-80EF-47AA-BE89-75B998169C3A
C6C8E8C1-5FFE-4738-9D93-127A7E5F031A
2FBAC95B-0BBF-49AD-B976-48DDA2C24213
5C2F7B20-00C4-44F3-8325-E0696CCFFAA4
DA6247E0-8AED-45F1-B6CE-1DBFE61FA65F
F6A40AE3-4FEE-47EC-BD5F-105B017A1CCF

POSSIBLE SECRETS
AC060003-328C-A28F-9846-5A8AA212661B
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
EA66C9CE-EFC9-4FB8-97CD-27987CCE52EB
B16A25B0-D718-40B2-83B9-A468E1F62574
1600BAE4-75B0-40E0-B6B1-95549FE0F912
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
16754893-135E-44ED-A23B-45BAD6E0551E
BD23EE10-44B0-4285-AF83-9DC7A6571F76
0ADE31FC-A7BA-44DB-8A7D-A1C2B3A4EEEB
410BD4A7-60C6-4F5C-BE84-894C9F48C283
A6EAEE37-9651-4F13-8012-CF437F59B9D9
8AA667FC-D2CA-4AA8-A093-017F5CD7A09B
26AC93A4-5513-4E31-9838-47227B1EE997
1DBAEDA1-5B43-46CC-A647-660084C416AD
E006A87D-F8A8-436D-9B5D-15EB45268D06

POSSIBLE SECRETS
7e7d89838e6873776dbd44c7b8df1a01
C3768173-C48A-4052-BC36-0514D8EB1651
22E77AC0-DEDC-4427-8A27-75CBBAFF06F2
151E4CCA-201A-4FDB-BB03-DD412D477701
0A2EBAA8-FE41-44CF-A00A-1B77094E9F6C
C4883E2A-249C-4D97-A48A-DD9BD902AA0C
FCA05FC6-0BFC-42CB-94AC-793B998FDA28
72ADC121-93FB-480E-BF67-1E0A44A04BEF
3FADF4B6-AFF3-4266-B4D7-370EF7AEDC37
40975133-74BC-4938-8431-0B033BEEA18A
D85DC299-91A1-47E9-8D5B-CBB24F5671C2
EAAD07D8-EF31-4A85-9D04-7380C1C6CD87
7d73d21f1bd82c9e5268b6dcf9fde2cb
B62A8A0C-CA4A-4D7D-918F-F22E4C90F8AB
C012957B-D27E-4BA7-9080-C829DCF75512

POSSIBLE SECRETS
4465A916-A1DF-4162-A6FE-71AC9525EB99
a0784d7a4716f3feb4f64e7f4b39bf04
07482A67-E0EE-4815-ABE8-A33D8637AC2D
465782CD-C947-454A-9A9E-A8DA5D811A54
8E22806C-E97E-4A50-AABA-5D14D0A73B26
2C665557-1089-490B-BBBB-1AE8E8596FA2
55602D93-B1FB-4D8C-A3EC-1C34812A1024
8E879E53-E839-486E-B3CE-796A5F0F8BBE
8858eb40-aee8-11e1-bb67-0002a5d5c51b
6ce895565c42ad7f2ec35a275979bac7
A0079B1E-638A-4B7A-83DC-CA42D09CB0FE
F6FFF60C-63BB-4C61-8B1D-807ED98C83C7
463F10A5-47DF-4DE3-BE85-BCC51BDDC27B
F729A155-67B3-42C0-B354-4E71E21D7E2C
D89565CD-97F7-4AD1-8BA4-0F80B5DDF7E6

POSSIBLE SECRETS
C964B071-CB96-4325-ADA7-D5547189ADD2
C3FFDD80-4DDB-48E7-B70A-B91CAAEB3D23
F5B126EC-1FB3-45CE-88CC-A4CF12FE0F58
C4919E53-A199-4677-97E7-D05BF61E3271
af60eb711bd85bc1e4d3e0a462e074eea428a8
9204C167-32A8-4819-9E02-924F07DFF438
0362648E-1EB1-4742-827A-53969714C3BB
C417DE09-A3A1-40AF-A89E-5AB4DB6CAD7E
663DAF9A-8023-44B9-9C88-B38AF79DD848
BDD49F6C-BDD6-4051-8AB5-70F6393AA229
C1F53456-C79E-47D3-AE82-BE53BE3C1AF0
47D0EFF9-BFD8-4997-9B73-A269B21E380E
001155e2fee767c4338ff03328a13b89
70DE35D6-98D1-4CED-B4CB-A1F6654DA7B9
10F72345-F1A2-48B8-A123-66B331024CC7

POSSIBLE SECRETS
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
EF8E107C-D190-444B-9B64-0F388B62A259
B553B924-EAA9-44C5-9B73-785BD1D03FF5
85053bf24bba75239b16a601d9387e17
8DB9AFF5-8E92-4CF5-9772-7CF667AD9FB2
9ED14654-00B8-472E-8525-12BC2E244CEC
3020C3FF-B5F3-48AE-91B8-D74F829709FB
46CEB1B9-9190-4D60-9E51-2DFFA983056F
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
e0b8a060-aee7-11e1-92f4-0002a5d5c51b
5CA79577-0278-41ED-AF6A-DC50EEF44F81
F0F7BAC8-A8DB-4F3F-9D17-CE19B183AF20
353D0C92-D29E-43E6-90E1-4780F6C3395A
A3FEB2FE-8B58-443B-A33C-F993F20C1584
9571AB07-8754-4DAE-AA9D-FE3AD6D95166

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853948
AC010001-F0A3-A691-444E-2A8AC9345D06
E4806626-14A3-491F-BA9F-128392FB55F8
BE9EF207-9389-48FD-8EE6-650D8AACDCBE
D5BC2BE2-0FF1-4249-9814-F9782CFE02FA
F0214539-A60C-4A02-BF9B-5F48A7C7E2F2
B6298B61-E56B-4D54-A337-89980BA4FD7E
115792089237316195423570985008687907853269984665640564039457584007908834671663
6e4000f0-b5a3-f393-efa9-e50e24dcca9e
DF39A1A9-A361-450F-AEE3-4DBC4FE8F5D4
8A0E38B2-1E7D-4DD4-84B5-14E553913590
42BD9A53-02F6-4274-83D6-56C2FBF6623A
46945BF7-8279-4338-A030-F327726EF64D
FF98B434-FD65-4CE6-A144-32497F318C42
91F1A608-73FE-40FA-B4FD-34621F268EC8

POSSIBLE SECRETS
DE87DCD4-63FE-4A92-9165-7148128952FB
B75EE24C-7B8F-4EBF-A83A-ED2306432B92
AFD15996-8300-435A-945F-66D96F29E7EF
E46A3CE1-F659-46A5-A1CB-537CCA17B09A
8638E52E-2293-4915-BAC3-CC33160C5A8D
6566B1E5-8E2B-480A-AE00-34C28C28AE49
F551B714-7DA3-4317-AEAE-3522BB3EB44E
030AD7AF-AB54-48ED-A2CE-BB0EB4476088
11F9E9AC-6EF0-404F-92E0-6551AAE343A1
D257E0BC-77B3-41B8-9CD2-D5C5F4B85FC8
16FDB44B-06C1-411B-BDF4-AB2650436C38
9DA8CCE1-4077-4BEB-9977-3722EBF49AA5
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
254CC25E-D7AF-4697-8F1A-5A365ECAFC39
7DD3F252-17A4-45CA-89E0-0805608C3AE7

POSSIBLE SECRETS
687C4DB3-48F0-4292-9EA4-579FF8DC50E4
EE25AB2B-2C35-4854-BF76-14E5E5D61E5E
C51F616D-14BE-4D95-A804-5EDAFE970F7A
1DEA8D7B-B9CE-4C26-8C85-FE8CF7433254
F3AE824D-126C-4769-B60F-1FB289C4B988
D0D15260-667E-4FBA-870F-C9338371B764
F021511B-A22F-474F-A8B0-27EA44680247
AE188411-0466-4BFD-B42D-E530898D8B34
E9A3746A-DCEE-4E3C-8865-019AF80FA1D2
7F1B5DCC-AE37-419E-8332-1EA48A680C50
C4E05CB3-4B19-4550-9DB7-7F75A23907FA
CC557D2F-CD9C-4D84-8FC4-67987C0DD29C
60866E62-D63B-4339-8827-FB80B90E82C3
A5B21064-5EDE-421F-9AB9-C1B54E46842C
9930039A-820E-4C7E-AE65-6E2AFABAFA66

POSSIBLE SECRETS
9BD0D0F7-8161-4A5A-B03B-B187DEE9E808
3CF81185-3B23-47A2-BC65-8B061ADB72EE
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
247084A0-2F76-4244-BE07-07C59366BC6F
07A20333-A45B-459D-A453-C741EE99FBAD
679BDA04-6C55-44AE-94A3-0F6F8CA533D0
4FF921E3-9516-4653-A09C-8D93EC7BBAD4
AC010001-328C-A28F-9846-5A8AA212661B
37E83A39-A095-44D2-A952-F7D07612DBF1
C0F79625-9BC4-45FF-B259-353823DD4098
1073FDA0-9A5C-418F-AAED-8F188CFADAFF
A47FFAF1-54D6-4AF8-85C6-FC3D2FF3CF67
560f1420-aee8-11e1-8184-0002a5d5c51b
219B5146-93CB-4E7E-AA1D-B59A533EEF22
E06A3658-2DB5-47E2-8184-30DB438336AD

POSSIBLE SECRETS
1C6F0AF1-7FDA-4E44-A5E8-DBE9590543FA
2C2B712D-D8F5-48B0-9C52-1FC626908D3D
DFEC21E0-AEEB-4734-966A-CF0AC69A3CD4
259E9745-5EE6-4224-8285-5BC784739BE9
174A2C6B-CCE0-49CB-9273-4BA9C709B735
2A92F323-9F7E-472B-AD89-13B700CD64E0
6B86B4D7-959E-446C-BF96-F1D984B73F36
953D897E-127B-4B09-BE2F-42C68006CF60
76AF6B55-9F19-41AA-8C68-A604218240CB
FB80A4D5-A9DD-4FC6-B916-A06282542FBF
1C9ACCEE-D6FB-4BD6-A02A-06C7F2BBFA8A
93CA8A53-6A6B-4E9A-B0A1-AC6F2AFB5C3F
7A9D235A-908A-42B9-B062-B2A4FCF96538
32670510020758816978083085130507043184471273380659243275938904335757337482424
EB6803FC-32C7-4080-8BAE-5E0B3D7A6B72

POSSIBLE SECRETS
CB49C0D3-C3A8-490E-993F-B2467B055730
E7512C62-2649-48C7-B869-CB3059DF67EB
8A06D51A-1424-41BE-8588-B7FD11934AA2
EAAC3FEF-AC19-4058-B54A-6CD1021EE9EF
DAF93813-F0D1-4976-B47A-7DB865E336AE
2D0B2EF1-7526-43AF-B024-B689454B04A8
02BF6F4F-5B37-4894-A3A4-3E120F0507CC
51199416-03DC-4AF7-9EE6-BADA6DB95840
B8382743-7C3E-4769-8CC1-CDFD32D108D1
838BAE83-B8EB-4C32-8622-36A0363C46F7
82d0e5086d9b08eda7f3f1875a6da7ba24bf7f60
12DF86DD-58E6-40E3-9566-51BE95FB5D62
CE3C3A25-2B55-4284-AAA1-560B798CD6A6
8662AC9B-CF99-4EFD-8118-297E27F4970F
614A3E02-42FA-40AB-A49E-649B3A239B36

POSSIBLE SECRETS
3F5D3122-0277-47D6-8A06-7BD5912F4080
115792089210356248762697446949407573530086143415290314195533631308867097853951
AC060001-328C-A28F-9846-5A8AA212661B
B73ADDEC-0F62-4DC9-AFEB-13B4EB869F78
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
27098703-204A-4BC3-91BD-AE1B94B6E3BB
4C9B6E84-629C-4AF1-B9F7-3F0DC584F3AF
A800DA1E-9252-45E2-8AAF-65C56C3708BF
1EAF7B39-D5D9-499C-9703-8E53AC6C2F6D
5A7616DF-2B80-47F0-94B1-5A528C2E3C78
803BAB26-508D-4AF0-B0A4-0934506D6535
8C32F26A-A13E-4817-B211-A9698A18F86E
5A872747-557B-4BA0-8897-E520F3A3CE58
8959DC72-0365-4A33-B2A2-95B4F31FCF26
992D52B2-0D6F-4C24-9ABB-35E177609A54

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
799ADE57-5939-49D0-ADBF-6D02B8A983A8
8D3DE695-D5D7-4717-9695-461EA7A8035E
6e400001-b5a3-f393-efa9-e50e24dcca9e
ecbe3980-c9a2-11e1-b1bd-0002a5d5c51b
6722E58C-CAB5-461F-8621-7E2D20590ADE
6D8B3D2A-D9F1-49C3-BED6-074763EF5371
D25E1991-9978-47CF-9F34-D4CE0C43BCD9
BAAFF3F2-C7D9-4E3A-859D-ADF6EBFEE5BD
C7E87651-4FE7-4998-A60E-4ED7AC26863F
98A8AEBD-13F8-4B50-975D-DADD58B1AAA2
90803790-433C-47C9-B946-45E51FA9F9C3
465B7F64-A7B7-4DE4-94A0-05A8C19D6C9F
0E0C15FD-4CFD-438E-82A7-315B50A69343
D5D6C848-3D3C-42A3-965F-7C0CA9CA5E90

POSSIBLE SECRETS
400A33E8-FE54-4D55-8E46-78B6AA5A36C0
F9599012-1105-4EBA-AC38-1123A5098FEE
4E36592D-9086-41BC-AC84-40E3A6278FF7
3CE5428A-E272-4403-A2CC-6A6E51971927
B494D126-F6BB-4377-93F4-559B10473CBB
bae8e37fc83441b16034566b
2FE44BAB-01DA-4431-B28F-09CFD5E7DED1
5a878b873ffd40f8ba554d369d8ca6b2
470fa2b4ae81cd56ecbcda9735803434cec591fa
9e0ae7d551d4e9897253179943eeb2ef
FD58F336-EFB8-4056-8486-661D23A0C36F
AA535843-4052-4D44-9A00-D3DFBC2ABD08
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
6d0ec0bb-c524-4d64-b793-8b7cad93f52b
597E4F21-7D9A-42B9-A23F-AF02C2060169

POSSIBLE SECRETS
6589B966-68E1-4D65-8688-469A4E98B2C3
76924311-3254-4069-845A-F6D56C848733
E6A3B121-0553-4B15-A877-B163EF9B9C3A
3FFB9103-4BB3-47A3-AC53-60F835EF2566
91BB82E1-26C5-44B7-A3E9-F696E72DBCB6
e3293c0b8b42d4368a5c42921339d7b0
48439561293906451759052585252797914202762949526041747995844080717082404635286
D6835B53-1DCA-4BC6-AD57-8BEF39E53497
76CD271C-8455-4387-9989-23BCD9352D55
C4AE3194-DE0C-46E8-876B-89599C2A8CEE
iGEn31zW0SvhbfXQHudVMbz9Mj07IFMzENzF8OG7io8=
51E64E1B-47BC-48B8-A413-CB8968306CC0
0E0A335B-7F30-4703-9522-D20AF721CEEB
81327CDF-688B-42AB-970A-30E5AE8801F4
BAB6562B-3474-4C38-9124-CD9AC20CB074

POSSIBLE SECRETS
F9476CAE-8364-4CC9-9D8D-6210D2B357B9
F905C88B-3818-4C27-A0DE-9F0DFCA0FB73
BBB940FD-BDC8-448D-9509-F73EADF9AD64
5C7A543D-DC71-476B-BD6C-9142031DD088
5D5A2031-60D9-47E5-87FA-497F5946DDE9
08FFF923-D2EA-43F8-8D6A-9AB881F8FB3C
F808D4B2-99F7-4D8B-B5FD-63D880837CDC
23456789abcdefghjkmnpqrstvwxyz
75E441F1-D736-48FE-A329-C41BF441FA06
E18A77DA-E0BB-45DA-9505-FD3F5380D113
F9A22A81-6249-41C2-A3BF-8A761820E635
C5E83A9A-E1B0-49FE-B935-969E1CAEB38D
86C4C5EA-123C-4AF2-B388-697471C48163
A255469B-07B9-4D2F-85BB-A93F52A7D306
1C14EEAE-0437-467D-A244-5CAA490BDEE0

POSSIBLE SECRETS
31F5D4A1-9A3F-40F7-980C-78DB2F1AA88E
542C6B78-F47E-4BDB-A8D2-3E542E6C31B2
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
AA927334-504B-4310-92B2-FB61783D0127
EA082E30-2438-4667-9D2E-B4CF42F08BA8
F28784E2-AC18-42FD-BDA4-AB0C6EAE87CF
3C23A883-F052-48CC-9956-21F88403A165
113A656A-6C98-4928-9CEF-AF247F9CA28D
MDNEjo1UtaMNDrLOKEwWc9y7nh3tfyso
F8E9DFFD-5073-476B-B305-502F6B2021FB
e6b49990-29ed-45be-8878-f0434687b6c7
420D447A-B332-4202-BB54-03CFC2D7D3B5
011DE8C9-98BA-43B9-9CBB-B4A91B895501
1411C8AB-AB20-43A8-B6D0-87F21641416E
E1D0E4F3-9563-4586-A817-C7B645B614E0

POSSIBLE SECRETS
883B18B0-C136-4604-A79B-3B27D89A3ED7
AC060002-328C-A28F-9846-5A8AA212661B
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
djJkX3FMckpnWkpOaVwhSDNtRQo=
991DDB4F-52AA-4816-A048-00528D14F17B
733F5C72-7097-4C1E-8D9B-D7FC5CBC10C8
7995E2D3-4B7F-48F1-882B-D2F088C39752
94C66D8E-00E1-4B6D-8C48-25FAE001DB02
B3AB0983-C1E3-4002-9DF0-30E0601B0F98
7C792E99-01AC-4834-8A7D-96166BF66D33
204B8BF8-565B-4FFC-8587-040C0BEB9640
CA37D3E7-A9C7-41BA-8738-0DFB7BB72490
36864200e0eaf5284d884a0e77d31646
4D4AB89F-43D0-4251-90E9-AB45622765D4
55066263022277343669578718895168534326250603453777594175500187360389116729240

POSSIBLE SECRETS
98CE53F3-BC41-43B2-A0E9-E83314D18A23
C8394491-4B88-46D2-9650-96BCDCB1850D
B52EA29C-4714-4000-96C9-C95D2DE9A2B9
E6865C17-9FEB-4E53-85F2-1E23F626FEC7
8D0B0DB3-5F5C-44C8-BEC7-EEFB06FA4D37
7613807B-636B-4FD2-93F6-CE96254932F7
7192EDB2-8A72-4554-B438-00A8C3C06C1C
115792089237316195423570985008687907852837564279074904382605163141518161494337
07234349-E8A3-44E8-869A-C730EDFCBCF9
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
900D85EB-E4F8-43A4-A7C5-C73AA4569AEB
02B371B8-897F-4910-B874-3B0A89003D0B
946896D6-9F0E-40BE-9811-648328073AE6
87DB7720-81AA-4C59-95C6-B110694FE08B
2B73D464-BCA7-49C6-BA45-3F3EE602B69E

POSSIBLE SECRETS
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
F2A9BAB8-9463-4D20-AF27-AA44D43EC063
88676305-56A9-4CEC-A505-CA6BD7DF45E4
ABB04E79-2216-4AFB-9D24-B18A07DDC377
165917A6-5BDC-4809-BD0E-F199D182C77C
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
D8A3ABB3-507F-46EE-9128-4E5D9F422FF5
530FE86E-943A-49D1-B1E6-C537B8BB1297
FFD5409A-36FA-4029-BACE-85A237A1705C
55C3C46D-007A-437E-87DC-8F95FBECCB2A
EA74F95B-3ADF-450E-9DF1-C2F7C4338B38
6160B0E2-D785-45DF-99A9-8F6F4AED7C58
D0035A36-08A6-4CCD-81F4-A54E4B5B376F
F44A861D-BF31-4DDE-BCD2-BABF8476057C
BDFFCA1A-9049-41BC-8613-908810FEC9B0

POSSIBLE SECRETS
4EC7CB42-11DA-4953-A7E2-DF7C0D998BB5
01DFD05E-347B-450E-9171-6F995A950C13
05B283F6-9E0F-4488-BEB7-910EF7DEF765
AC010002-F0A3-A691-444E-2A8AC9345D06
42305953-22CD-4B4A-B719-F7CDBC71FC41
6F6409DD-9EEA-41FE-A40D-EF1AEE30F048
59DBC749-1578-4D60-92A4-89294CEB436B
1BC84983-8E66-4A77-B8AB-96E3C345D9BB
3ECB90F5-1149-4451-A7FF-2DEEB31BB1C0
A7C26346-155B-4A24-9DFD-6F63B39EE6D1
717912EC-D825-49F1-AE9B-EFA8005CB2F2
E6CEF703-B48A-4A9D-9BB9-57F1EAB3D30B
DA8D750B-58D9-4C6E-9431-6FC5AA27B02D
7CFD064D-BA7F-48E6-944D-024C47079CE0
E8A427AF-913E-43D1-8985-816351FDE195

POSSIBLE SECRETS
618E0150-A28B-4D62-B81C-2A1B9E485E76
9b775e13fa5161847f6cc6b5009c8967
2A09C3AD-91AD-4867-83B5-CD821865F206
786555E8-7735-4791-A7A5-D7399A699FBC
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1A7EFEB5-EAD8-45AE-A051-A753DFAD2DF9
48AD8C43-9232-4B9A-80A4-9B4A6682DE35
6699AB0C-34E5-4C84-9A98-B93F35D1EB50
DC98D838-C575-4909-93D3-E52690691A14
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
B3CFD8B0-B8BF-486A-92E4-B25DFCD39385
F3A745D9-757D-422E-B936-8DC66630F518
EE75AC85-9908-4393-8ECF-649D5F65C918
C25790A9-8AB0-4C95-9903-9E333E5F6EC7
F2365F9B-45F8-458E-AB68-FC4A46C9C182

POSSIBLE SECRETS
0494D82D-3380-484B-A6D7-F3C19FA5B204
85529C0A-1E53-4C9A-B2F5-67ED416C80BD
1F3A283E-814A-4F04-8A1A-F524E5263BAA
3120C2BA-9ACC-4A2F-B0C5-6A8854E0DED3
5F36DC8E-15C9-4B9C-93CC-526C06487B0F
6ADD584E-9E89-4F04-AE0A-1163E93DAFF1
43CA281C-8E65-443E-A16B-2D637AD45656
44619D7A-9BCA-4A33-9161-AAFF779C29B1
08D41427-3CA0-4B5D-96FE-356241458EEE
4AA18A52-F4E1-419D-9F8B-E8850FE4D6F0
FD50B04F-4FE0-490B-A41A-F74E359E75DC
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
355EF5A0-9F63-4ED6-A1D6-CB723C3692B8
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
62303C8F-AAB2-49AE-9896-1D4808229FAA

POSSIBLE SECRETS
CC1CDAF0-A87B-4343-B550-05BFD188E3E6
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
db5b55e0-aee7-11e1-965e-0002a5d5c51b
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
21FF9FFE-E1B7-4481-86E6-EDF92CF4D590
35D3BF0A-90C8-4F4B-B72D-E5CD70B49952
3071c8717539de5d5353f4c8cd59a032
6e4000f1-b5a3-f393-efa9-e50e24dcca9e
A90015FE-C9F3-49E0-A207-BAB89ED92CF6
6F8BD7E6-EB34-4E3B-AF98-B32D41293606
737E7ABC-0702-4596-A895-C9DC1426A11A
951F0718-B704-4297-9C34-61CC2089F27B
F38A921B-0ADD-4900-8890-CEED9689BB6F
36134250956749795798585127919587881956611106672985015071877198253568414405109
D25885B2-A8FD-4B20-A255-CCAE770BBE75

POSSIBLE SECRETS
9A2C1E15-D938-4858-B6DB-81AA8D708DC7
4d0bf320-aee8-11e1-a0d9-0002a5d5c51b
1BA1EC3E-F6C5-46B4-BC92-D8C8E162859A
ECF9E7B9-581E-4AFF-81A6-AAD1A1044AFA
FF927441-255B-4AB9-AA46-A2694D776195
3E80361E-6E33-4766-BA02-003281C95531
928EF113-0128-4297-94EE-5D550489F314
CBF5D3FF-D665-4611-9003-3C968865A12C
D7E3F50F-9416-412D-9407-3B1C5F95A1D0
5668CBFD-FF36-4657-8599-F2C33B5364A6
54D142A9-E7F9-4CB1-8707-10C8285D5544
57B27902-8423-44F2-A6CD-309CF416F945
8B66AD6A-5B7A-498E-9086-961AEB2B81F7
4144DED4-D75C-4631-BE0B-AD810CA18EB0
5488271C-8178-4D94-8374-987FA5A856F8

POSSIBLE SECRETS
13AD1D2E-1093-4480-9A56-7AC9DEF84CD3
CDF6CFA9-93AE-4D29-A84B-CD985EB23975
8F5D1D1A-9006-4F20-9953-3946D9DD9EA1
C776E3E6-1736-4D1D-993F-D7F335F5B5E4
CA417CD1-183C-481C-A4E2-3A931402F81A
557FB6DB-6972-4695-BFB2-120499CF011A
D114EF98-A75B-4AEA-83E2-6E53A1DECBC8
067EAB5E-6EB7-4B4A-BF78-1D2911E91C2D

PLAYSTORE INFORMATION

Title: Kardia

Score: 4.7359242 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.alivecor.aliveecg

Developer Details: AliveCor Inc., AliveCor+Inc., None, http://www.alivecor.com, support@alivecor.com,

Release Date: Oct 3, 2013 **Privacy Policy:** Privacy link

Description:

Kardia works with the FDA-cleared KardiaMobile, KardiaMobile 6L, or KardiaBand personal EKG devices, which can detect the most common arrhythmias in just 30 seconds. The Kardia app is designed to make managing heart care from home easier than ever, giving you the ability to seamlessly record EKGs, share heart data with your doctor remotely, keep track of your health history, and more. Capture a medical-grade EKG with your Kardia device anytime, anywhere—no patches, wires, or gels required. Get an immediate result from Kardia's Instant Analysis of normal, possible atrial fibrillation, bradycardia, or tachycardia. For additional analysis, you can choose to send the recording to your physician or to one of our partners for a Clinician Review by a cardiologist (US, Australia only) or cardiac care physiologist (UK, Ireland only).

The Kardia system is recommended by leading cardiologists and used by people around the world for accurate EKG recordings. Track your heart health data from home with the medical accuracy your doctor can trust. NOTE: This app requires KardiaMobile, KardiaMobile 6L, or KardiaBand hardware to record an EKG. Get your Kardia device now at alivecor.com.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:21:13	Generating Hashes	OK
2025-08-29 19:21:19	Extracting APK	OK
2025-08-29 19:21:19	Unzipping	OK
2025-08-29 19:21:33	Parsing APK with androguard	OK
2025-08-29 19:21:35	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:21:36	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:21:42	Parsing AndroidManifest.xml	OK
2025-08-29 19:21:42	Extracting Manifest Data	OK

2025-08-29 19:21:42	Manifest Analysis Started	OK
2025-08-29 19:21:42	Reading Network Security config from network_security_config.xml	OK
2025-08-29 19:21:42	Parsing Network Security config	OK
2025-08-29 19:21:42	Performing Static Analysis on: Kardia (com.alivecor.aliveecg)	OK
2025-08-29 19:21:43	Fetching Details from Play Store: com.alivecor.aliveecg	OK
2025-08-29 19:21:45	Checking for Malware Permissions	OK
2025-08-29 19:21:45	Fetching icon path	OK
2025-08-29 19:21:45	Library Binary Analysis Started	OK
2025-08-29 19:21:52	Reading Code Signing Certificate	OK
2025-08-29 19:21:53	Running APKiD 2.1.5	OK
2025-08-29 19:22:08	Detecting Trackers	OK

2025-08-29 19:22:15	Decompiling APK to Java with JADX	OK
2025-08-29 19:22:52	Converting DEX to Smali	OK
2025-08-29 19:22:52	Code Analysis Started on - java_source	OK
2025-08-29 19:23:03	Android SBOM Analysis Completed	OK
2025-08-29 19:23:18	Android SAST Completed	OK
2025-08-29 19:23:18	Android API Analysis Started	OK
2025-08-29 19:23:32	Android API Analysis Completed	OK
2025-08-29 19:23:33	Android Permission Mapping Started	OK
2025-08-29 19:24:02	Android Permission Mapping Completed	OK
2025-08-29 19:24:42	Android Behaviour Analysis Started	OK
2025-08-29 19:25:14	Android Behaviour Analysis Completed	OK

2025-08-29 19:25:14	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:26:20	Email and URL Extraction Completed	OK
2025-08-29 19:26:20	Extracting String data from APK	OK
2025-08-29 19:26:23	Extracting String data from Code	OK
2025-08-29 19:26:23	Extracting String values and entropies from Code	OK
2025-08-29 19:27:08	Performing Malware check on extracted domains	OK
2025-08-29 19:27:18	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.