MOBSF

ANDROID STATIC ANALYSIS REPORT

Eko (4.16.0)

File Name:	com.ekodevices.android_5015550.apk
Package Name:	com.ekodevices.android
Scan Date:	Aug. 29, 2025, 10:01 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	17	3	2	1

FILE INFORMATION

File Name: com.ekodevices.android_5015550.apk
Size: 105.59MB
MD5: c43d8acf6ae1d2a32262f291b62050f9
SHA1: 70abb010867b1c51d13a49968e2f67ac63aaf789
SHA256: 16ac04d2bfc8f0391d8ea7a9156cc20d52a2210d2b80cece9c46f1c80129fa51

APP INFORMATION

App Name: Eko
Package Name: com.ekodevices.android
Main Activity: com.ekodevices.app.presentation.journey.splash.SplashActivity
Target SDK: 34
Min SDK: 30
Max SDK:
Android Version Name: 4.16.0

Android Version Code: 5015550

APP COMPONENTS

Activities: 17
Services: 13
Receivers: 17
Providers: 3
Exported Activities: 2
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=01, ST=CA, L=San Fransisco, O=Eko Devices
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-02-04 04:29:29+00:00
Valid To: 2042-01-29 04:29:29+00:00
Issuer: C=01, ST=CA, L=San Fransisco, O=Eko Devices
Serial Number: 0x5470d6e9
Hash Algorithm: sha256
md5: 8a5856578df83161ec40de4f50f04f64
sha1: fb1363a5ad8a01f57f45a458964a471346170dad
sha256: be506b7ec52c3b6fc2329cdfafaae4a1639f24b711cb81214ba5b9ac4f3e64eb
sha512: 8de097b32ceae6d0bdccbb09abc5c7c31908f6be48cb16df6dc2b6bc6d46a37a7c805424dc1050b97765a3be54a1e08ff1b28098123318cbb13a99f096596fa5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: aee06df92d8c0b0b678d14dfff77ce549dab202deae2efc64ffc1d99463493f4
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.

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.ekodevices.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.

APKID ANALYSIS

FILE	DETAILS
c43d8acf6ae1d2a32262f291b62050f9.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

FILE	DETAILS
classes.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Anti-VM Code: Build.FINGERPRINT check Build.MANUFACTURER check Compiler: unknown (please file detection issue!)
classes2.dex	FINDINGS / DETAILS yara_issue: yara issue - dex file recognized by apkid but not yara module Anti-VM Code: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check Compiler: unknown (please file detection issue!)

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ekodevices.app.presentation.journey.dashboard.DashboardActivity	Schemes: https://, Hosts: deeplinks.ekohealth.com, Paths: /eko-app-android,

NETWORK SECURITY

HIGH: **4** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	ekohealth.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
2	google.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
3	mixpanel.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
4	privacyshield.gov	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (com.ekodevices.app.presentation.journey.dashboard.DashboardActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Broadcast Receiver (com.ekodevices.app.service.ServiceStartReceiver) 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.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	D3/a.java N3/b.java N3/j.java O3/A.java P3/z.java Q3/W.java Q3/Z.java Q3/b0.java Q4/i.java R6/c.java V/c.java V/o.java W3/o.java W3/p.java com/ekodevices/app/service/BaseEkoDeviceConnectionService$startDeviceJobs$1$invokeSuspend$lambda$8$$inlined$launchIn$4.java com/ekohealth/filter/g0.java n4/C2995a.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteQueryBuilder.java o4/C3035a.java org/slf4j/helpers/j.java r5/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	H3/M.java H3/W.java com/mixpanel/android/mpmetrics/MPDbAdapter.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/database/SQLiteDatabase.java
3	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	J0/a.java X5/b.java com/ekodevices/app/presentation/journey/dashboard/userAccountDetailsFlow/behavior/AccountDetailsStepCountryOfResidenceBehavior.java com/ekodevices/app/presentation/journey/dashboard/userAccountDetailsFlow/behavior/AccountDetailsStepPracticeBehavior.java com/ekodevices/app/presentation/journey/dashboard/userAccountDetailsFlow/behavior/AccountDetailsStepProviderBehavior.java com/ekodevices/app/presentation/journey/dashboard/userAccountDetailsFlow/behavior/AccountDetailsStepSpecialtyBehavior.java com/ekodevices/ekodata/core/Authenticator.java com/ekodevices/ekodata/core/CustomInterceptor.java com/ekodevices/ekodata/model/user/SignUpRequestDTO.java com/ekodevices/ekodata/model/user/User.java com/ekodevices/ekodata/model/user/UserRequest.java com/ekodevices/library/ota/Duo15OTAHandler.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCa

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-14	che.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java e2/d.java l2/InterfaceC2948c.java v5/C3284b.java w5/C3303e.java w5/w.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Q6/c.java Q6/d.java Q6/g.java Q6/h.java
5	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	O5/a.java com/revenuecat/purchases/common/UtilsKt.java h7/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	net/sqlcipher/database/SupportHelper.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ekodevices/ekoutils/device/model/EURecording.java
8	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	M0/C0743r0.java U0/r.java
9	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	y2/C3336f.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Q4/v.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/ekodevices/library/device/mock/MockWavDevice.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	h0/C2728h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	h0/C2728h.java
00022	Open a file from given absolute path of the file	file	coil/disk/a.java com/ekodevices/app/presentation/journey/dashboard/firmwareUpdate/FirmwareUpdateFragment.java com/ekodevices/app/presentation/journey/onboarding/viewModel/UserViewModel$downloadFirmware$2.java com/ekodevices/ekoutils/device/model/EURecording.java com/ekodevices/library/EDFileHelper.java com/ekodevices/library/device/EDDevice$Companion$decompressAsync$1.java com/ekodevices/library/device/EDDevice.java com/ekodevices/library/ota/EDOTAManager.java com/ekodevices/library/utils/EDBGAutoRecordManager.java com/ekodevices/library/utils/EDCEAutoRecordManager$startRecording$2$1.java p2/q.java v5/f.java y2/C3336f.java y2/C3337g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B5/a.java N1/b.java U6/u.java com/ekodevices/app/presentation/base/DeviceConnectionBaseActivity$firmwareDownload$2$1$1$1.java com/ekodevices/library/EDFileHelper.java com/ekodevices/library/device/EDDevice$Companion$decompressAsync$1.java com/ekodevices/library/device/EDDevice$startBulkAssetTransferSendAsync$1.java com/ekodevices/library/device/EDDevice.java com/ekodevices/library/utils/ConvertUtils.java com/ekodevices/library/utils/SignalQualityClassifier.java com/ekodevices/library/utils/ZipDecompressor.java com/revenuecat/purchases/common/FileHelper.java v5/f.java y2/C3336f.java y2/C3337g.java z5/C3403e.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ekodevices/app/common/BaseActivity$checkAppForceUpdateAvailable$1$1.java com/ekodevices/app/presentation/journey/confirmation/EmailConfirmationFragment.java com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/menusettings/AppSettingsFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/onboarding/EkoAppUpdateActivity.java com/ekodevices/app/service/BaseEkoDeviceConnectionService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ekodevices/app/presentation/journey/confirmation/EmailConfirmationFragment.java com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/menusettings/AppSettingsFragment$showEnablePostNotificationDialog$1.java
00036	Get resource file from res/raw directory	reflection	com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnableBackgroundActivityDialog$1.java com/ekodevices/app/presentation/journey/dashboard/BaseReviewRecordingFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/presentation/journey/menusettings/AppSettingsFragment$showEnablePostNotificationDialog$1.java com/ekodevices/app/service/BaseEkoDeviceConnectionService.java k2/C2805e.java
00162	Create InetSocketAddress object and connecting to it	socket	Q6/b.java Q6/h.java g7/b.java
00163	Create new Socket and connecting to it	socket	Q6/b.java Q6/h.java g7/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java
00004	Get filename and put it to JSON object	file collection	com/mixpanel/android/mpmetrics/MPDbAdapter.java
00078	Get the network operator name	collection telephony	com/mixpanel/android/mpmetrics/j.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	H0/a.java
00096	Connect to a URL and set request method	command network	K0/i.java com/mixpanel/android/util/a.java com/revenuecat/purchases/common/HTTPClient.java y2/C3332b.java
00030	Connect to the remote server through the given URL	network	K0/i.java y2/C3332b.java
00094	Connect to a URL and read data from it	command network	K0/i.java com/mixpanel/android/util/a.java y5/C3341a.java
00091	Retrieve data from broadcast	collection	com/ekodevices/library/ota/EDOTAManager.java
00089	Connect to a URL and receive input stream from the server	command network	K0/i.java com/mixpanel/android/util/a.java com/revenuecat/purchases/common/HTTPClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	K0/i.java L3/d.java com/mixpanel/android/util/a.java com/revenuecat/purchases/common/HTTPClient.java
00108	Read the input stream from given URL	network command	K0/i.java com/mixpanel/android/util/a.java
00014	Read file into a stream and put it into a JSON object	file	B5/a.java v5/f.java
00024	Write file after Base64 decoding	reflection file	p2/q.java
00132	Query The ISO country code	telephony collection	I0/H.java
00005	Get absolute path of file and put it to JSON object	file	v5/f.java
00189	Get the content of a SMS message	sms	com/ekodevices/library/device/mock/MockWavDevice.java
00188	Get the address of a SMS message	sms	com/ekodevices/library/device/mock/MockWavDevice.java
00200	Query data from the contact list	collection contact	com/ekodevices/library/device/mock/MockWavDevice.java
00201	Query data from the call log	collection calllog	com/ekodevices/library/device/mock/MockWavDevice.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ekodevices/library/device/mock/MockWavDevice.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://ekoandroidappproduction.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/938782148052/namespaces/firebase:fetch?key=AIzaSyB4Yl4AFURgd95fezstiLf_9v4dfM9bzdc is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'ab_test_direct_to_playback': '{"name":"dtp_experiment_1","id":"A","value":true}', 'ab_test_force_trial_paywall': '{"name":"","id":"","value":true}', 'battery_status_notification_critical': '5', 'battery_status_notification_low': '20', 'confirm_email_reminder_in_days': '3', 'core500_skip_assets': '["1.0.10","1.0.11"]', 'eas_udi_description': '(01)00850010298030(8012)', 'eas_udi_version': '6.5.0', 'eleft_udi_description': '(01)00850010298146(8012)', 'eleft_udi_version': '7.5.0', 'emas_udi_description': '(01)00850010298184(8012)', 'emas_udi_version': '1.2.0', 'extended_bluetooth_mtu_unsupported_devices': '{"devices":["SM-T290"]}', 'in_us': 'true', 'is_background_connection_enabled': 'false', 'is_distortion_popup_enabled': 'false', 'mixpanel_debug_trace': '0', 'mixpanel_debug_whitelist': '[]', 'new_user_rating_reminder_in_days': '10', 'play_from_headphones_unsupported_devices': '{"devices": []}', 'rating_enable': 'true', 'rating_reminder_in_days': '10', 'rollout_percentage': '100', 'single_recording_auto_record_operating_parameters_core2': '{ "windowsToStartRecordingCount": 8, "averageProbability": 0.07, "onBodyProbability": 0.07, "offBodyProbability": 0.07, "resetWindowingProbability": 0.07, "offBodySqiCount": 6, "idleDwellMilliseconds": 5000, "impedanceOnBodyMilliseconds": 3000 }', 'single_recording_auto_record_operating_parameters_core500': '{ "windowsToStartRecordingCount": 8, "averageProbability": 0.07, "onBodyProbability": 0.07, "offBodyProbability": 0.07, "resetWindowingProbability": 0.07, "offBodySqiCount": 6, "idleDwellMilliseconds": 5000, "impedanceOnBodyMilliseconds": 3000 }', 'single_recording_auto_record_operating_parameters_duo': '{ "windowsToStartRecordingCount": 8, "averageProbability": 0.07, "onBodyProbability": 0.07, "offBodyProbability": 0.07, "resetWindowingProbability": 0.07, "offBodySqiCount": 6, "idleDwellMilliseconds": 5000, "impedanceOnBodyMilliseconds": 3000 }'}, 'state': 'UPDATE', 'templateVersion': '80'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
fonts.gstatic.com	ok	**IP:** 172.217.215.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.revenuecat.com	ok	**IP:** 52.203.57.188 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.zetetic.net	ok	**IP:** 18.238.96.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.ekodevices.com	ok	**IP:** 52.71.68.231 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.google.com	ok	**IP:** 173.194.219.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
dashboard.ekodevices.com	ok	**IP:** 52.71.68.231 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.mixpanel.com	ok	**IP:** 35.186.241.51 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 172.253.124.157 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
assets.pawwalls.com	ok	**IP:** 18.238.96.88 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.ekohealth.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 54.243.244.245 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
shop.ekohealth.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
support.ekohealth.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ekoandroidappproduction.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api-paywalls.revenuecat.com	ok	**IP:** 54.160.110.226 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 18.238.109.64 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
revenuecat.com	ok	**IP:** 18.238.109.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	O3/l.java
support@ekodevices.com	com/ekodevices/app/presentation/journey/confirmation/EmailConfirmationFragment.java
support@ekohealth.com	com/ekodevices/app/presentation/journey/menusettings/CustomerSupportFragment.java
user@organization.com name@email.com support@ekohealth.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "1b902cc0357146ed98761bbc3ffc7482"
"event_key_api_http_method" : "apiHTTPMethod"
"event_key_api_name" : "apiName"
"event_key_api_response_code" : "apiResponseCode"
"event_key_auto_record_notification" : "autoRecordNotification"
"event_key_ble_hci_status" : "bleHciStatus"
"event_key_tc_log_type" : "LogType"
"firebase_database_url" : "https://ekoandroidappproduction.firebaseio.com"
"google_api_key" : "AIzaSyB4Yl4AFURgd95fezstiLf_9v4dfM9bzdc"
"google_crash_reporting_api_key" : "AIzaSyB4Yl4AFURgd95fezstiLf_9v4dfM9bzdc"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"verify_credentials_continue_dc_button" : "Continue"
CD54FB7B-61A4-40A4-A34A-E6CFEAE11AA6
40B90C02-9306-4DCF-94BD-4CC71515026A
128C9930-5AD6-41FD-BE20-19BE7E82602E

POSSIBLE SECRETS
60a5bda51486b21538d5313a
605c94521fa5e5688fd6985c
00060000-F8CE-11E4-ABF4-0002A5D5C51B
BA9C5360-9999-11E3-966F-0002A5D5C51B
BA0E9DCD-EA10-4AA3-9190-B848598F2F75
C2148E84-CB1F-4A05-9ED0-832A1E9FB336
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
EA73858B-9185-4958-9A7E-7204C3E198E6
E6EA3564-D144-4DD3-A884-C9AAA3BFCC19
5BF6E500-9999-11E3-A116-0002A5D5C51B
72BB4346-7487-4552-8779-121DF2435162
7BB44072-14F7-42C2-B0DE-2A340909B180
34696772-1597-429D-A2E3-5C036F9F39DE
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
56dde76ae7c0aba813742a8d3ceb2a77
600554E8-C6A4-4218-8488-39697AFC7D6A
ba9c5360-9999-11e3-966f-0002a5d5c51b
2AF120D7-4D40-4FF1-96C6-D803455A3959
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
41966176-C762-428C-98DA-2A371AAE1C49
04e6fc4788aa8ec9882df9c7bf20d299
ded8aba3feafca13c7b0ab450cc13e9e
B532B98C-7D69-4CDB-B7D0-297A77478790
5bf6e500-9999-11e3-a116-0002a5d5c51b
C320D257-D7BE-46AC-9A37-7A4EDFA84BCE
12CAE281-318D-4C0D-A2AF-176639A5C54D
19BE0323-442C-4F80-A0A0-5B7C204FB883
CC719BF7-7AAA-47CE-9CD7-29F223B4B61E
75F0A9DA-183D-4CE6-BC9B-334812D40A1E

POSSIBLE SECRETS
00060001-F8CE-11E4-ABF4-0002A5D5C51B
7BB44072-14F7-42C2-B0DE-2A340909B181
B532B98B-7D69-4CDB-B7D0-297A77478790
37C205D6-3D62-43CD-81FB-1E7931950022
C2DE8ABD-959B-4F00-BD84-556A0F45EE28
5181942b9ebc31ce68dacb56c16fd79f
F1DE0EF3-6E8F-4FA6-B538-5BD318BDBCCB
31DDCAB1-2788-4AF0-B019-9307CEBFAF53
580B41EC-243F-42D6-A922-8CD6DEF5F941
8CED7DE2-6D15-4E8C-932D-C2BE048146DA
C2D4F30F-E149-43F5-B1B5-B31E7C2EF5D4
00060000-f8ce-11e4-abf4-0002a5d5c51b
00060001-f8ce-11e4-abf4-0002a5d5c51b
611CA734-3C3D-4FF7-B908-3587E127DB41

PLAYSTORE INFORMATION

Title: Eko: Digital Stethoscopes

Score: 4.7083335 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ekodevices.android

Developer Details: Eko Health, Inc, Eko+Health,+Inc, None, https://ekohealth.com, contact@ekohealth.com,

Release Date: Feb 3, 2017 **Privacy Policy:** Privacy link

Description:

The Eko App turns every patient encounter into an early detection opportunity for heart and lung disease. It fits seamlessly into your physical exam workflow when connected to a compatible digital stethoscope. Use the Eko App to: - Flag the presence or absence of murmurs. - Flag the presence of AFib*, tachycardia, and bradycardia. - Listen wirelessly using the Bluetooth-enabled device of your choice. - Record, play back, annotate, and save stethoscope sounds and ECG*. - Build patient profiles to flag changes in a patient's condition across visits. - Securely store exam recordings for future reference. - Generate and share PDF reports with trusted colleagues or upload to compatible EHRs. - Aid in medical education and patient engagement. *Available with the CORE 500™ Digital Stethoscope. Select features may require a paid Eko+ membership. Requires Android 11 and up. Visit ekohealth.com to learn more about compatible devices. Have questions or feedback? Contact us at support@ekohealth.com. The Services are for informational purposes only and should not replace advice from a licensed healthcare provider for any medical condition or treatment. Please consult a licensed and qualified health care provider before making any medical decisions.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:01:25	Generating Hashes	OK
2025-08-29 22:01:25	Extracting APK	OK
2025-08-29 22:01:25	Unzipping	OK
2025-08-29 22:01:25	Parsing APK with androguard	OK

2025-08-29 22:01:26	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:01:26	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:01:28	Parsing AndroidManifest.xml	OK
2025-08-29 22:01:28	Extracting Manifest Data	OK
2025-08-29 22:01:28	Manifest Analysis Started	OK
2025-08-29 22:01:28	Reading Network Security config from network_security_config.xml	OK
2025-08-29 22:01:28	Parsing Network Security config	OK
2025-08-29 22:01:28	Performing Static Analysis on: Eko (com.ekodevices.android)	OK
2025-08-29 22:01:29	Fetching Details from Play Store: com.ekodevices.android	OK
2025-08-29 22:01:30	Checking for Malware Permissions	OK
2025-08-29 22:01:30	Fetching icon path	OK

2025-08-29 22:01:30	Library Binary Analysis Started	OK
2025-08-29 22:01:30	Reading Code Signing Certificate	OK
2025-08-29 22:01:30	Running APKiD 2.1.5	OK
2025-08-29 22:01:33	Detecting Trackers	OK
2025-08-29 22:01:36	Decompiling APK to Java with JADX	OK
2025-08-29 22:01:55	Converting DEX to Smali	OK
2025-08-29 22:01:55	Code Analysis Started on - java_source	OK
2025-08-29 22:01:59	Android SBOM Analysis Completed	OK
2025-08-29 22:02:10	Android SAST Completed	OK
2025-08-29 22:02:10	Android API Analysis Started	OK

2025-08-29 22:02:22	Android API Analysis Completed	OK
2025-08-29 22:02:23	Android Permission Mapping Started	OK
2025-08-29 22:02:34	Android Permission Mapping Completed	OK
2025-08-29 22:02:35	Android Behaviour Analysis Started	OK
2025-08-29 22:02:46	Android Behaviour Analysis Completed	OK
2025-08-29 22:02:46	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:02:50	Email and URL Extraction Completed	OK
2025-08-29 22:02:50	Extracting String data from APK	OK
2025-08-29 22:02:50	Extracting String data from Code	OK
2025-08-29 22:02:50	Extracting String values and entropies from Code	OK
2025-08-29 22:02:54	Performing Malware check on extracted domains	OK

2025-08-29 22:02:56	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.