MOBSF

ANDROID STATIC ANALYSIS REPORT

Endel (3.120.882)

File Name:	com.endel.endel_312088200.apk
Package Name:	com.endel.endel
Scan Date:	Aug. 29, 2025, 10:04 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	36	4	2	1

FILE INFORMATION

File Name: com.endel.endel_312088200.apk
Size: 31.24MB
MD5: 1a8cd9abfe9da7b8ba547a193bd6a98d
SHA1: 7ef2e4bfbff9399068ba7226238f30ed8ef998a1
SHA256: a1394215573adcc4b854af3bfb660169767837b38ebce0b8a3d8d8fbdf8ab178

APP INFORMATION

App Name: Endel
Package Name: com.endel.endel
Main Activity: com.endel.endel.use_cases.root.RootActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 3.120.882

Android Version Code: 312088200

APP COMPONENTS

Activities: 18
Services: 24
Receivers: 21
Providers: 5
Exported Activities: 7
Exported Services: 5
Exported Receivers: 10
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-01-31 17:54:01+00:00
Valid To: 2049-01-31 17:54:01+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xcf1c6897da641903c0a83c882c461dbc24150eba
Hash Algorithm: sha256
md5: 898ced216fcf2b94d85d41d9b94778ff
sha1: 8fa309c9714708a69821ad6de7d554db116d3037
sha256: 9289c30cee30ca40278504d5d375c93ace705ebf57a444a9e30a3132d3345d19
sha512: 7295fe5137a7fab8b9822b1c83a36e7698fb9e6a8fef202634024e68e05fb6018a5b495db7abc72c0959d7ed8e0ea7a4d00054d32be5d96364f992733263f73e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: da1db2f75ab2a4216a75ffc6596e80ba0ee2f6a22186a3e83b7b54be9af6fad3
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.endel.endel.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

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

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.endel.endel.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>1a8cd9abfe9da7b8ba547a193bd6a98d.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
SIM operator check
network operator name check
device ID check
ro.kernel.qemu 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>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.TAGS check
possible VM 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>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.endel.endel,
com.endel.endel.use_cases.root.RootActivity	Schemes: http://, https://, @string/APP_SCHEME://, Hosts: endel.page.link,
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: 1 | WARNING: 1 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.
2	*	high	Base config is configured to trust user installed certificates.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 23 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config_beta]	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.facebook.FacebookActivity) 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.facebook.CustomTabActivity) 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	Service (com.endel.endel.services.wear.ListenerServiceFromWear) 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.
6	Service (com.endel.endel.services.audio.service.MediaService) 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.
7	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) 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.
8	Broadcast Receiver (com.endel.endel.bl.notification.NotificationsReceiver) 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.
9	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
10	Broadcast Receiver (com.endel.endel.bl.broadcast.BluetoothA2DPReceiver) 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
11	Broadcast Receiver (com.onesignal.FCMBroadcastReceiver) 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.
12	Activity (com.onesignal.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Broadcast Receiver (com.onesignal.NotificationDismissReceiver) 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.
14	Broadcast Receiver (com.onesignal.BootUpReceiver) 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.
15	Broadcast Receiver (com.onesignal.UpgradeReceiver) 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	Activity (com.onesignal.NotificationOpenedReceiver) 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
17	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) 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.
18	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.
19	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.
20	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.
21	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
22	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.
23	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.
24	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.
25	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 3 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	Z7/m.java com/appsflyer/internal/AFb1zSDK.java com/revenuecat/purchases/common/UtilsKt.java s4/C3592a.java x8/C4086b.java
				B/f.java B4/k.java B6/C0752y2.java Ba/a.java Ba/b.java C7/g.java D/a.java D/b.java D/c.java D/d.java D0/m.java D6/a.java E/a.java E/e.java E/f.java E/g.java E/h.java E/j.java E/k.java E/l.java E/m.java E/p.java E/r.java E/s.java E/u.java E/v.java E4/a.java E6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				F6/A.java F6/AbstractServiceC0877x.java F6/C0867m.java F6/C0868n.java F6/C0874u.java F6/C0875v.java F6/L.java F7/C0903z.java G0/B.java G0/C0920a.java G0/w.java G6/B1.java G6/C0967o.java G6/D1.java G6/E1.java G6/K0.java G6/L.java G6/M.java G6/O.java G6/v1.java G6/w1.java H1/C.java H8/B.java H8/C1007g.java H8/D.java H8/G.java H8/k.java H8/x.java I/C1014d.java I/C1019i.java I/I.java I/P.java I0/b.java I8/a.java J/a.java J6/h.java J8/c.java J8/f.java K/c.java K/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				K/h.java K0/l.java Kc/a.java L/d.java L/f.java L/g.java L/h.java L/l.java M5/C1319u.java M6/a.java N0/b.java N5/l.java N9/E.java O0/A.java O0/B.java O0/C.java O0/D.java O0/x.java O5/g.java P0/g.java R/i.java R/u.java S7/o.java T0/j.java U3/C1507c.java U3/C1510f.java U3/G.java U3/m.java V/AbstractC1554b.java V/C1574w.java V/K.java V/M.java V/Q.java V/Y.java Va/j.java X3/l.java Y/f.java Y3/e.java Y3/f.java Z/k.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	Z5/g.java Z7/u.java a0/C1764q.java a0/I.java a4/C1783a.java a8/C1804a.java b6/AbstractC1904A.java b6/AbstractC1912b.java b6/C1906C.java b6/C1907D.java b6/C1913c.java b6/C1921k.java b6/C1935y.java b6/ServiceConnectionC1934x.java c4/f.java c4/i.java c4/l.java c6/C2011E.java c6/C2019f.java c6/C2022i.java c6/C2023j.java c6/J.java c6/m.java c6/v.java c6/z.java c7/C2033i.java com/adjust/sdk/Logger.java com/airbnb/lottie/LottieAnimationView.java com/amplitude/api/f.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1nSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1sSDK.java com/appsflyer/internal/AFd1tSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1uSDK.java com/appsflyer/internal/AFf1bSDK.java com/apptimize/Apptimize.java com/apptimize/ax.java com/apptimize/bd.java com/apptimize/bu.java com/apptimize/ge.java com/apptimize/ml.java com/apptimize/sb.java com/apptimize/wg.java com/apptimize/xt.java com/endel/endel/bl/broadcast/BluetoothA2DPReceiver.java com/endel/endel/common/analytics/AnalyticsImpl$setupSubscribers$21.java com/endel/endel/services/sony/SonyForegroundService.java com/onesignal/C2211e.java com/onesignal/C2251r1.java com/onesignal/JobIntentService.java com/revenuecat/purchases/common/DefaultLogHandler.java com/samsung/android/sdk/healthdata/HealthDataObserver.java com/samsung/android/sdk/healthdata/HealthDataStore.java com/samsung/android/sdk/healthdata/HealthPermissionManager.java com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java com/samsung/android/sdk/internal/healthdata/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthdata/StreamUtil.java e7/C2425a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e7/C2426b.java e7/f.java e7/k.java e7/o.java e7/r.java e7/s.java e8/C2428a.java f4/C2473a.java f7/C2482B.java g0/C2528a.java g6/C2562a.java h/LayoutInflaterFactory2C2605d.java h/l.java h/n.java h/p.java i6/AbstractC2750a.java j6/C2846b.java jc/C2867e.java k6/g.java k6/r.java k6/s.java k8/g.java m/g.java n/MenuItemC3135c.java n4/C3241c.java o/C3321u.java o/C3324x.java o/L.java o/d0.java o/g0.java o/h0.java o/m0.java o/n0.java o/w0.java o/x0.java o/z0.java o0/C3327a.java o6/d.java org/joda/time/tz/DateTimeZoneBuilder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/joda/time/tz/ZoneInfoCompiler.java p7/f.java q0/C3400b.java s0/AbstractC3567a.java s1/C3572e.java s4/C3594c.java t4/D.java t4/E.java t4/y.java u6/B.java v0/C3801b.java v8/b.java v9/C3883b.java w0/c.java w7/C3935A.java w7/C3938D.java x0/C3992a.java x5/l.java x7/AbstractC4058E.java x7/C4082x.java x7/J.java x7/L.java x7/O.java x7/Y.java x7/j0.java x8/C4086b.java y/C4100d.java y0/AbstractServiceC4105b.java y8/C4175c.java
				z7/AbstractC4195l.java z7/C4188c.java z7/C4254g.java z7/o.java W3/g.java com/amplitude/api/AmplitudeClient.java com/endel/endel/models/FirebaseMessageSender.java com/endel/endel/models/NotificationKt.java com/endel/endel/specs/AnalyticsProfileItem.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/endel/endel/specs/DeeplinksModel.java com/endel/endel/specs/SubtitleFormat.java com/endel/wear_shared/specs/MediaSource.java com/onesignal/AbstractC2274v0.java com/onesignal/B0.java com/onesignal/U1.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/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/B.java defpackage/C.java defpackage/E.java defpackage/I0.java defpackage/InterfaceC1877b0.java defpackage/InterfaceC3010l.java defpackage/InterfaceC4180z.java defpackage/X.java defpackage/o0.java defpackage/v0.java defpackage/z0.java l5/C3046a.java
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	Y2/f1.java com/apptimize/an.java
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	B6/K6.java F6/C0875v.java N4/C1379q0.java V7/a.java Y2/C1696n.java Y2/f1.java Z7/j.java com/adjust/sdk/Util.java com/appsflyer/internal/AFa1wSDK.java com/appsflyer/internal/AFb1pSDK.java com/apptimize/qt.java com/apptimize/vf.java com/apptimize/vh.java com/onesignal/OSUtils.java g8/h.java hb/C2705o.java p5/F.java s5/C3596b.java xb/AbstractC4092a.java xb/C4093b.java yb/C4179a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	a4/C1792j.java g4/C2552b.java t4/D.java
7	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	B6/C0656m.java B6/C0663m6.java B6/C0667n2.java B6/C0742x.java B6/U6.java I4/M.java I4/W.java L0/a.java S7/p.java com/amplitude/api/i.java com/apptimize/nb.java com/onesignal/C2284y1.java t9/k.java
8	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	G0/B.java com/apptimize/q_.java x8/C4087c.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	B6/K6.java U3/C1508d.java c4/l.java com/appsflyer/internal/AFb1zSDK.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ic/C2779d.java ic/C2780e.java ic/C2785j.java ic/C2786k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	F7/C0887i.java c7/v.java f7/C2498g.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	w5/i.java
13	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	u5/C3764a.java
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/onesignal/d2.java
15	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/d2.java
16	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/apptimize/ov.java
17	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. 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	g8/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	G0/B.java H1/r.java H7/f.java I0/a.java L0/b.java L2/C1210i0.java N9/E.java Q7/d.java W7/f.java com/appsflyer/internal/AFe1uSDK.java com/apptimize/et.java com/apptimize/ge.java com/apptimize/ml.java com/apptimize/or.java com/apptimize/q_.java com/apptimize/x.java e7/f.java e7/k.java e7/o.java f2/C2462i.java i0/l.java p1/g.java p1/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	B6/K6.java c6/C2020g.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/InstallReferrerHuawei.java com/adjust/sdk/a.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1iSDK.java com/karumi/dexter/listener/multi/SnackbarOnAnyDeniedMultiplePermissionsListener.java com/karumi/dexter/listener/single/SnackbarOnDeniedPermissionListener.java com/onesignal/OSUtils.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java h4/C2620a.java o/m0.java
00130	Get the current WIFI information	wifi collection	com/adjust/sdk/MacAddressUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	B6/C0613g4.java B6/C0663m6.java B6/K6.java B6/P4.java E2/j.java G3/e.java G6/w1.java Y1/B.java Y1/l.java Y2/C1696n.java b3/C1893b.java c6/C2020g.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1oSDK.java com/karumi/dexter/listener/multi/SnackbarOnAnyDeniedMultiplePermissionsListener.java com/karumi/dexter/listener/single/SnackbarOnDeniedPermissionListener.java com/onesignal/OSUtils.java com/onesignal/PermissionsActivity.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java t4/C3637c.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	G3/e.java Y2/C1696n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	Ac/k.java F7/l.java G0/B.java H1/r.java H7/f.java I0/c.java L/f.java L/l.java L7/e.java N7/a.java U3/C1510f.java c4/l.java com/adjust/sdk/PreinstallUtil.java com/appsflyer/internal/AFa1jSDK.java com/appsflyer/internal/AFe1uSDK.java com/apptimize/p0.java com/revenuecat/purchases/common/FileHelper.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java d4/j.java g4/C2551a.java i0/l.java l4/k.java nc/r.java o0/C3327a.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java p1/g.java p1/h.java rb/h.java rb/j.java x8/C4087c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	L5/s.java W3/g.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/apptimize/qt.java com/onesignal/D1.java com/revenuecat/purchases/common/HTTPClient.java p1/C3364b.java y4/C4142d.java y8/C4175c.java
00089	Connect to a URL and receive input stream from the server	command network	H1/C.java L5/s.java W3/g.java com/amplitude/api/g.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/apptimize/qt.java com/onesignal/D1.java com/revenuecat/purchases/common/HTTPClient.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java s4/C3594c.java y4/C4142d.java y8/C4175c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	H1/C.java L5/s.java W3/g.java Z5/f.java com/amplitude/api/g.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/appsflyer/internal/AFd1lSDK.java com/apptimize/qt.java com/onesignal/D1.java com/revenuecat/purchases/common/HTTPClient.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java y4/C4142d.java y8/C4175c.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/i.java com/apptimize/nb.java com/onesignal/C2206c0.java com/onesignal/H.java com/onesignal/Z.java com/onesignal/r.java
00092	Send broadcast	command	com/onesignal/Z.java
00034	Query the current data network type	collection network	com/adjust/sdk/Util.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	B6/P4.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/onesignal/F0.java com/onesignal/FCMBroadcastReceiver.java t4/I.java x1/x0.java
00094	Connect to a URL and read data from it	command network	H1/C.java K7/a.java L5/s.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	N9/p.java S/d.java com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00012	Read data and put it into a buffer stream	file	H1/r.java U3/C1510f.java c4/l.java com/apptimize/p0.java o0/C3327a.java
00132	Query The ISO country code	telephony collection	M5/Z.java com/amplitude/api/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	H1/C.java L5/s.java com/appsflyer/internal/AFa1uSDK.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java p1/C3364b.java
00108	Read the input stream from given URL	network command	B6/B2.java B6/V4.java H1/C.java L5/s.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00191	Get messages in the SMS inbox	sms	com/adjust/sdk/a.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1iSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java o/m0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	b3/C1893b.java c6/C2020g.java com/onesignal/OSUtils.java com/onesignal/PermissionsActivity.java
00079	Hide the current app's icon	evasion	d1/C2301g.java
00014	Read file into a stream and put it into a JSON object	file	H7/f.java N7/a.java com/appsflyer/internal/AFe1uSDK.java d4/j.java g4/C2551a.java l4/k.java x8/C4087c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	H7/f.java com/appsflyer/internal/AFe1uSDK.java com/apptimize/ge.java com/apptimize/x.java
00072	Write HTTP input stream into a file	command network file	H1/C.java
00004	Get filename and put it to JSON object	file collection	com/apptimize/ov.java com/apptimize/x.java d4/C2326f.java l4/c.java p4/C3375a.java
00125	Check if the given file path exist	file	d4/C2326f.java
00078	Get the network operator name	collection telephony	com/amplitude/api/k.java com/appsflyer/internal/AFa1iSDK.java com/onesignal/OSUtils.java
00162	Create InetSocketAddress object and connecting to it	socket	ic/C2778c.java ic/C2786k.java
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java com/apptimize/p0.java ic/C2778c.java ic/C2786k.java
00137	Get last known location of the device	location collection	com/amplitude/api/k.java
00115	Get last known location of the device	collection location	com/amplitude/api/k.java h/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00023	Start another application from current application	reflection control	com/onesignal/C2251r1.java
00189	Get the content of a SMS message	sms	S/d.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	S/d.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	S/d.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	S/d.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	S/d.java com/appsflyer/internal/AFf1hSDK.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00153	Send binary data over HTTP	http	com/apptimize/qt.java
00114	Create a secure socket connection to the proxy address	network command	dc/C2354f.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1eSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	W/w.java
00147	Get the time of current location	collection location	h/p.java
00075	Get location of the device	collection location	h/p.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/AmplitudeClient.java
00003	Put the compressed bitmap data into JSON object	camera	X3/l.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://endel-ios.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/104792671767/namespaces/firebase:fetch?key=AIzaSyBYj43KD7_SggQ98W6_sbfAqlFG7emfFMo is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'state': 'EMPTY_CONFIG', 'templateVersion': '1'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	8/44	android.permission.FOREGROUND_SERVICE, android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api-production.endel.io	ok	**IP:** 18.238.109.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.googleadservices.com	ok	**IP:** 64.233.185.154 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.revenuecat.com	ok	**IP:** 34.227.123.75 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
endel.zendesk.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
endel-ios.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
share.endel.io	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
app.adjust.com	ok	**IP:** 185.151.204.10 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 74.125.136.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
endel.io	ok	**IP:** 18.238.96.59 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sattr.s	ok	No Geolocation information available.
teams.endel.io	ok	**IP:** 18.238.96.41 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	ok	**IP:** 64.233.177.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
s.endel.io	ok	**IP:** 18.238.109.35 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.43 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
accounts.google.com	ok	**IP:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
endel-static.s3-eu-west-1.amazonaws.com	ok	**IP:** 3.5.65.172 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.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
api2.amplitude.com	ok	**IP:** 52.88.145.168 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.16.160.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
hub.samsungapps.com	ok	**IP:** 34.240.53.86 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 34.227.123.75 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
static.endel.io	ok	**IP:** 18.238.109.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
code.endel.io	ok	**IP:** 18.238.96.129 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
payment.endel.io	ok	**IP:** 18.238.109.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.googleapis.com	ok	**IP:** 108.177.122.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sapp.s	ok	No Geolocation information available.
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
endel-static.s3.eu-west-1.amazonaws.com	ok	**IP:** 3.5.68.175 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 18.238.109.116 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api-staging.endel.io	ok	**IP:** 18.238.96.40 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
google.com	ok	**IP:** 142.250.9.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 64.233.176.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c6/u.java
ystem_banner_offer_1@2x.png	F1/H.java
u000ez+zm4bb@f.i8gm	com/apptimize/j8.java
h_@y.fpw4 u001aq@5g.jh u0004@kk.en	com/apptimize/h7.java
t@h3llpt.a5e_ u0012@xmz.bj u0014@b.an u0001q@ssbg.njv u00005gc@r.ew acrwyf@e.w_ u007f@r.zg	com/apptimize/sn.java

EMAIL	FILE
u0010-@ggd.tu	com/apptimize/nt.java
ask@endel.io collaboratewith@endel.io	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Apptimize	Analytics	https://reports.exodus-privacy.eu.org/trackers/135
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "24a9d72eb82e487387d60574987ee7a0"
"firebase_database_url" : "https://endel-ios.firebaseio.com"
"google_api_key" : "AIzaSyBYj43KD7_SggQ98W6_sbfAqlFG7emfFMo"
"google_crash_reporting_api_key" : "AIzaSyBYj43KD7_SggQ98W6_sbfAqlFG7emfFMo"
"introductory_flow.activity.creative_session" : "Create"
"onboardingV2.service_auth.already_allowed" : "Allowed"
"onboardingV2.service_auth.restricted" : "Restricted"
"onboardingV3.first_session.outro.focus.button" : "Continue"
"onboardingV3.first_session.outro.relax.button" : "Continue"
"onboardingV3.first_session.outro.sleep.button" : "Continue"
"scenarios.activity.creative_session" : "Create"
"survey.focus.summary.comment1_author" : "VDP"
"survey.sleep.summary.comment1_author" : "Rasha-tan"

POSSIBLE SECRETS
"survey.sleep.summary.comment2_author" : "smrtnarosa"
"survey.sleep.summary.comment3_author" : "grzgrzgrx"
"survey.summary.comment2_author" : "PeterOng"
"survey.summary.comment3_author" : "octosoup"
"tutorial.session_2.ok_button_title" : "Continue"
"tutorial.session_3.ok_button_title" : "Close"
"tutorial.session_4.ok_button_title" : "Continue"
"tutorial.session_5.ok_button_title" : "Continue"
"tutorial.session_5.title" : "Hey,"
"user.password" : "Password"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

POSSIBLE SECRETS
308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d01010505003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f696431223020060 92a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303232393031333334365a170d3335303731373031333334365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964312 2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d 6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81b bfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2cb3f28 4a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e24 7553311c46b9af76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a381fc3081f9301d0603551d0e0416041448 5900563d272c46ae118605a47419ac09ca8c113081c90603551d230481c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b3009 0603550406130255533113301106035504081 30a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964312230200600 92a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100 7aaf968ceb50c441055118d0daabaf0 15b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824b656dbe4dc22 40912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea5603b2c540dbd 7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430e ea7c26a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
49f946663a8deb7054212b8adda248c6
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
af60eb711bd85bc1e4d3e0a462e074eea428a8

POSSIBLE SECRETS
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
F76ACB01-7CAB-495F-BB1A-E664598FD77F
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
36864200e0eaf5284d884a0e77d31646
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f3118301606035504 0a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d303930383331323135323136 5a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f3118301606035504 0a130f46616365626f6f6b204d6f62696c653111300f060355040b13084 6616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c2 07d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de20 18ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864 886f70d010104050003818100 5ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483 998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b4 2bd928a2
64206ac54d4bc07bb6ad301c781f2741

POSSIBLE SECRETS
F76ACB02-7CAB-495F-BB1A-E664598FD77F
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
F76ACB00-7CAB-495F-BB1A-E664598FD77F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
76c13020-fe8f-416a-b4c3-ee59d3ef95dc
c682b8144a8dd52bc1ad63
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
e82733991c20e3c5771d3dac97efc0ee
956C7B26-D49A-4BA8-B03F-B17D393CB6E2
5eb5a37e-b458-11e3-ac11-000c2940e62c
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d01010405003081943 10b30090603550406130255533113301106035504081 30a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30 820120300d06092a864886f70d01010105000382010d00308201080282010100 9c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc 01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37 a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350e ec535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604 144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b30 0906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964312302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100572551b8d93a1f73de0f6d469f86d ad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12 d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc0596 17cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8 399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
76c13021-fe8f-416a-b4c3-ee59d3ef95dc
F76ACB03-7CAB-495F-BB1A-E664598FD77F

POSSIBLE SECRETS
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
c103703e120ae8cc73c9248622f3cd1e
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
ac797ca3-7556-4a36-a56c-1e37383943c5
fbd390c59f36c4f38022ba3b3db1589d
a0784d7a4716f3feb4f64e7f4b39bf04

POSSIBLE SECRETS

308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d313130363232313232323531325a170d333831313037313232323531325a3081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b5231143012060355040813 0b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031 30c53616d73756e672043657274312530230609 2a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d20995a79c0daad6300c0603551d130405300301 01ff300d06092a864886f70d0101050500038201010032960 1fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299db4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512dfb28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c810158

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS
308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f7265613113301106035504070c0a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531335a170d3338313130373132323531335a3081a2310b300906035504061302 4b52311430120603550408130b536f757468204b6f7265613113301106035504070c0a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b300906035504061302 4b52311430120603550408130b536f757468204b6f7265613113301106035504070 130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900e5eff0a8f66d92b3300c0603551d13040530030101ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
308201e53082014ea00302010202044f54468b300d06092a864886f70d01010505003037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d3132303330353034353232375a170d3432303232363034353232375a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f69642044656275673081 9f300d06092a864886f70d010101050003818d00308189028181008a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c59905032798273462bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001300d06092a864886f70d0101050500038181000512992268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122
b2f7f966-d8cc-11e4-bed1-df8f05be55ba

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Endel: Focus, Relax & Sleep

Score: 4.4324327 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.endel.endel

Developer Details: Endel Sound GmbH, Endel+Sound+GmbH, None, https://endel.io/, ask@endel.io,

Release Date: May 29, 2019 **Privacy Policy:** Privacy link

Description:

Focus, relax, and sleep through the power of sound. Endel creates AI-powered sounds designed to support your everyday life. Backed by science, and enjoyed by millions worldwide. Endel is powered by its patented core AI technology. It takes inputs like location, environment, and heart rate, to create the optimal personalized soundscape. This happens on the fly and allows Endel to reconnect your state with your circadian rhythm • Relax – calms your mind to create feelings of comfort and safety • Focus – boosts your productivity by helping you concentrate for longer • Sleep – soothes you into a deep sleep with soft, gentle sounds • Recovery – revives your wellbeing with sounds engineered to lower anxiety • Study – improves concentration and keeps you calm whilst studying or working • Move – boosts performance and enjoyment while walking, hiking, and running Endel collaborations Alongside the much-loved Endel classics, Endel works with innovative artists and thinkers to create original experiences. Grimes, Miguel, Alan Watts, and Richie Hawtin aka Plastikman have all contributed to the growing catalog of soundscapes –– with more on the way. • James Blake: Wind Down – designed to support a healthy routine before bed – easing from evening to sleep with supportive sounds. • Grimes: AI Lullaby – original vocals and music created by Grimes. Scientifically engineered for sleep • Miguel: Clarity Trip – made for mindful walks, hikes or runs. With original adaptive sounds from Grammy-winning artist, Miguel. • Alan Watts: Wiggly Wisdom – soothing and motivating spoken word soundscape. Infused with the playful wisdom of Alan Watts • Plastikman: Deeper Focus – a deep focus techno soundscape created with Richie Hawtin Use at home, work, or on the move to relax, concentrate, and minimize distractions and brain fatigue. All modes are available offline. Using Wear OS app you can see the current and upcoming biological rhythms phases right on your watch face without opening the app. Use them as an energy compass to navigate the day. ENDEL SUBSCRIPTION You can subscribe to Endel, choosing from the following plans: – 1 month – 12 months – Lifetime The subscription automatically renews unless auto-renewal is turned off at least 24 hours before the end of the current period. Payment will be charged to your account at confirmation of purchase. Account will be charged for renewal within 24 hours of the end of the current period, and the cost of the renewal will be provided. Subscriptions may be managed by the user. Auto-renewal may be turned off by going to the user's Account Settings after purchase. No cancellation of the current subscription is allowed during active subscription period. Any unused portion of a free trial period, if offered, will be forfeited when the user purchases a subscription to that publication. For more information: Terms of Use - https://endel.zendesk.com/hc/en-us/articles/360003558200 Privacy Policy - https://endel.zendesk.com/hc/en-us/articles/360003562619

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:04:24	Generating Hashes	OK
2025-08-29 22:04:24	Extracting APK	OK
2025-08-29 22:04:24	Unzipping	OK
2025-08-29 22:04:25	Parsing APK with androguard	OK
2025-08-29 22:04:25	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:04:25	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:04:27	Parsing AndroidManifest.xml	OK
2025-08-29 22:04:27	Extracting Manifest Data	OK
2025-08-29 22:04:27	Manifest Analysis Started	OK

2025-08-29 22:04:28	Reading Network Security config from network_security_config_beta.xml	OK
2025-08-29 22:04:28	Parsing Network Security config	OK
2025-08-29 22:04:28	Performing Static Analysis on: Endel (com.endel.endel)	OK
2025-08-29 22:04:28	Fetching Details from Play Store: com.endel.endel	OK
2025-08-29 22:04:29	Checking for Malware Permissions	OK
2025-08-29 22:04:29	Fetching icon path	OK
2025-08-29 22:04:29	Library Binary Analysis Started	OK
2025-08-29 22:04:29	Reading Code Signing Certificate	OK
2025-08-29 22:04:30	Running APKiD 2.1.5	OK
2025-08-29 22:04:34	Detecting Trackers	OK
2025-08-29 22:04:37	Decompiling APK to Java with JADX	OK

2025-08-29 22:04:52	Converting DEX to Smali	OK
2025-08-29 22:04:52	Code Analysis Started on - java_source	OK
2025-08-29 22:04:57	Android SBOM Analysis Completed	OK
2025-08-29 22:05:06	Android SAST Completed	OK
2025-08-29 22:05:06	Android API Analysis Started	OK
2025-08-29 22:05:15	Android API Analysis Completed	OK
2025-08-29 22:05:16	Android Permission Mapping Started	OK
2025-08-29 22:05:24	Android Permission Mapping Completed	OK
2025-08-29 22:05:24	Android Behaviour Analysis Started	OK
2025-08-29 22:05:36	Android Behaviour Analysis Completed	OK
2025-08-29 22:05:36	Extracting Emails and URLs from Source Code	OK

2025-08-29 22:05:41	Email and URL Extraction Completed	OK
2025-08-29 22:05:41	Extracting String data from APK	OK
2025-08-29 22:05:41	Extracting String data from Code	OK
2025-08-29 22:05:41	Extracting String values and entropies from Code	OK
2025-08-29 22:05:45	Performing Malware check on extracted domains	OK
2025-08-29 22:05:48	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.