MOBSF

ANDROID STATIC ANALYSIS REPORT

Balance (1.156.0)

File Name:	com.elevatelabs.geonosis_811.apk
Package Name:	com.elevatelabs.geonosis
Scan Date:	Aug. 29, 2025, 10:02 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	16	4	2	1

FILE INFORMATION

File Name: com.elevatelabs.geonosis_811.apk
Size: 99.83MB
MD5: 95cd5eb6c3291049d145c546c727c247
SHA1: 243385cf755bf3041848378ff43f79838ae5b93d
SHA256: b0315172d44ad69354d24ec524fa84ff2450683aefec1aa32b19aa4fe9a0f3aa

APP INFORMATION

App Name: Balance
Package Name: com.elevatelabs.geonosis
Main Activity: com.elevatelabs.geonosis.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.156.0

Android Version Code: 811

APP COMPONENTS

Activities: 18
Services: 10
Receivers: 12
Providers: 3
Exported Activities: 3
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-03 18:46:04+00:00
Valid To: 2050-12-03 18:46:04+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xdfbb3d40bb610d9dbfa5c5fb407f2017be0c9017
Hash Algorithm: sha256
md5: 05e5c206ee665e118440a3427b0ecafc
sha1: e887de511b03829eaa0e5a3778c50b2b2d7253e0
sha256: e34bb5b324c89c2229714ff4740ebd7a161b869c3fd665e8ccabf72c431d58cb
sha512: 4982079775f421442368aa0d83e7b2d74c0d479d39293b1105dda61e1242b4ce4e1b9ff95bfc69b53c32e06c68435db0655db8b92d9b7ac315d0e82be85b6996
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 971da70d675203213a6d094c8d71d1c0b1282bba3efd31fb527453611cf2014b
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.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".
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
BIND_GET_INSTALL_REFERRER_SERVICE	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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.elevatelabs.geonosis.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
95cd5eb6c3291049d145c546c727c247.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
SIM operator check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.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>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.elevatelabs.geonosis.MainActivity	Schemes: balanceapp://,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.elevatelabs.geonosis,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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.
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 (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.
6	Activity (androidx.activity.ComponentActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (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: 6 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/C0047k.java A3/d.java A3/e.java A9/v0.java Ac/D.java B1/AbstractC0163a0.java B1/B0.java B1/C0164b.java B1/C0192t.java B1/O.java B1/w0.java B1/x0.java B3/a.java B6/b.java B8/CallableC0261x0.java B8/F1.java B8/J1.java B8/M.java B8/M0.java B8/RunnableC0234l1.java B8/RunnableC0253t0.java B8/U0.java B8/V.java B8/X0.java Bc/n.java C4/a.java C9/a.java Cc/d.java Cc/e.java D4/C0307d.java D4/m.java D6/B.java D6/h.java D6/u.java D8/a.java D9/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				D9/d.java E3/C0344i.java E3/M.java E8/a.java E9/c.java F9/d.java Fb/h.java G1/c.java G2/b.java G8/b.java Gc/l.java H1/r.java H5/v.java H6/d.java I0/C0530i1.java I0/K.java I1/d.java I8/b.java I9/a.java I9/b.java K0/b.java L1/d.java N/B.java N/t.java Nc/a.java P3/e.java P6/a.java Q0/z.java Q5/e.java Q7/c.java S1/a.java S5/K0.java S5/N.java T1/b.java T1/c.java T1/g.java T4/g.java T7/a.java T8/e.java T9/b.java T9/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				U1/A.java U1/AnimationAnimationListenerC0868g.java U1/C.java U1/C0867f.java U1/C0871j.java U1/C0883w.java U1/b0.java U5/C0899j.java U8/a.java U9/b.java V/C0935r0.java V1/c.java V2/w.java V6/d.java V6/j.java V7/g.java V7/j.java V9/c.java W0/n.java W0/v.java W8/g.java X8/d.java Y3/i.java a8/c.java a8/d.java a8/i.java a9/C1224c.java a9/C1226e.java aa/C1229b.java b7/RunnableC1367b.java b8/C1377b.java b8/C1379d.java b8/C1381f.java b8/C1386k.java b8/C1387l.java b8/HandlerC1380e.java b8/RunnableC1384i.java b8/ServiceConnectionC1385j.java c1/C1414a.java c8/f.java c8/h.java

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	c8/k.java e3/n.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/ui/debugview/models/InternalDebugRevenueCatScreenViewModel$refreshInfo$1.java com/revenuecat/purchases/ui/debugview/models/InternalDebugRevenueCatScreenViewModel.java com/singular/sdk/Singular.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/ExternalAIFAHelper.java com/singular/sdk/internal/LicenseChecker.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularInstance.java com/singular/sdk/internal/SingularLog.java com/singular/sdk/internal/SingularRequestHandler.java e8/C1912A.java e8/C1914a.java e8/C1920g.java e8/HandlerC1919f.java e8/r.java ea/C1949a.java f2/C1974b.java f3/C1975a.java f3/c.java f8/AbstractC2024e.java f8/AbstractC2036q.java f8/BinderC2009F.java f8/C2011H.java f8/C2014K.java f8/C2016M.java f8/C2027h.java f8/HandlerC2008E.java f8/t.java g1/C2058b.java g6/G.java g6/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				g6/o.java g6/q.java g6/w.java h/AbstractC2112g.java h6/C2156i.java h6/k.java h6/o.java h6/t.java i3/b.java j/j.java j/p.java j/s.java j0/e.java j1/c.java j2/C2252C.java j2/C2262c.java j2/C2273n.java j6/AbstractC2341i.java j6/C2343k.java j6/C2344l.java j8/C2349a.java k3/C2377d.java k6/C2399e.java k8/AbstractC2403b.java k8/AbstractC2405d.java l1/e.java l2/C2426c.java l2/C2432i.java l3/C2436d.java l4/e.java l9/AbstractC2456b.java l9/C2458d.java l9/C2460f.java m/h.java m/i.java m6/C2499d.java n/MenuC2531m.java n/ViewOnKeyListenerC2525g.java nb/C2573a.java o/C2622s0.java o/C2628v0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o/C2631x.java o/C2633y.java o/L0.java o/M.java o/N0.java o/T.java o/Y0.java o/Z.java o6/AbstractC2663f.java o6/AbstractC2664g.java o6/C2659b.java o6/C2667j.java o8/d.java o8/e.java oa/C2675a.java oa/C2676b.java pa/C2761c.java pa/RunnableC2760b.java pa/l.java q3/C2835a.java q3/C2836b.java q8/d.java q8/f.java r5/C2893a.java r6/b.java s0/j.java s1/AbstractC2955b.java s1/o.java s2/c.java s9/d.java t1/C3008g.java t2/H.java t2/Y.java t2/k0.java t2/q0.java t4/C3046G.java t4/C3070m.java t7/C3095c.java ta/B.java ta/C3138l.java ta/C3139m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ta/H.java ta/J.java ta/N.java ta/P.java ta/Q.java ta/V.java ta/w.java u1/AbstractC3180c.java u2/C3186a.java u6/C3265B.java u6/C3267D.java u6/C3270c.java u6/C3276i.java u6/s.java u9/C3292a.java uc/b.java v8/h.java v8/i.java v9/C3405b.java v9/C3406c.java v9/C3407d.java v9/e.java va/C3409b.java va/C3410c.java va/C3411d.java va/C3415h.java w1/i.java w6/C3508c.java x1/AbstractC3561a.java x3/c.java x9/b.java y9/h.java y9/i.java y9/j.java y9/k.java y9/m.java y9/o.java y9/q.java y9/r.java y9/s.java y9/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y9/v.java y9/x.java z0/c.java z9/C3747d.java z9/g.java z9/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	A7/a.java C3/b.java L3/a.java Q/P0.java V/X.java V0/I.java bo/app/u4.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/singular/sdk/internal/BaseApi.java com/singular/sdk/internal/Constants.java d5/C1750i.java pc/Q.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	B8/J1.java I8/b.java Q5/d.java Y3/n.java h6/m.java o6/AbstractC2668k.java
4	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	B8/J1.java D6/u.java D9/d.java E7/a0.java F6/a.java I0/C0520f0.java Sb/a.java Sb/b.java Tb/a.java Y3/b.java Y3/k.java b7/C1374i.java bo/app/e1.java c7/RunnableC1454o.java ka/d.java o9/C2674a.java oa/C2679e.java oa/C2680f.java pa/g.java pa/l.java r8/AbstractC2922a.java
5	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	C4/a.java u6/K.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	I0/C0525h.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	L3/j.java S5/C0800u0.java W0/n.java bo/app/e.java bo/app/g6.java bo/app/h4.java bo/app/i0.java bo/app/j6.java bo/app/k0.java bo/app/l.java bo/app/m.java bo/app/o1.java bo/app/p6.java bo/app/q3.java bo/app/w4.java bo/app/y.java bo/app/y0.java bo/app/y5.java g6/C2089c.java g6/G.java m6/j.java s6/C2979b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	B8/C0223i.java B8/F1.java B8/G0.java B8/H.java B8/O1.java C4/a.java D4/C0307d.java V6/d.java V6/h.java V6/i.java V6/j.java W6/f.java W6/l.java W6/m.java com/singular/sdk/internal/OfflineEventsMigrator.java com/singular/sdk/internal/SQLitePersistentQueue.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	U9/b.java a/AbstractC1131a.java com/revenuecat/purchases/common/UtilsKt.java com/singular/sdk/internal/Utils.java k8/AbstractC2403b.java u6/AbstractC3280m.java y9/h.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a9/C1226e.java y9/h.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Bc/e.java Bc/h.java Bc/m.java Bc/n.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	B8/U.java S7/u.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java f3/C1975a.java
00109	Connect to a URL and get the response code	network command	B8/RunnableC0253t0.java B8/U.java S7/u.java V6/j.java V9/c.java a8/c.java com/revenuecat/purchases/common/HTTPClient.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java g6/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B8/r1.java C6/a.java D9/c.java E7/I.java G3/i.java Gc/t.java I7/j.java M1/A.java M1/F.java O1/e.java P1/i.java Q3/h.java Q5/d.java S7/C0815g.java S7/D.java T/C0.java U5/p.java V2/i.java Y3/i.java bo/app/l0.java c7/C1450k.java com/revenuecat/purchases/common/FileHelper.java f3/d.java h6/k.java o6/AbstractC2668k.java s2/c.java s2/h.java s6/C2978a.java tc/w.java u1/AbstractC3180c.java u6/C3276i.java v3/g.java y9/e.java y9/h.java y9/o.java z9/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	S7/u.java V6/j.java com/revenuecat/purchases/common/HTTPClient.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java f3/C1975a.java g6/n.java j9/f.java
00089	Connect to a URL and receive input stream from the server	command network	B8/RunnableC0234l1.java S7/u.java V6/j.java V9/c.java com/revenuecat/purchases/common/HTTPClient.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularRequestHandler.java g6/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	B8/J1.java B8/U0.java B8/X0.java D6/C0325a.java E5/C0351c.java F6/a.java I0/C0535k0.java P4/g.java Q7/c.java S5/C0788o.java U3/h.java W0/n.java com/appboy/Appboy.java com/elevatelabs/geonosis/features/notifications/NotificationAlarmReceiver.java f3/c.java j2/C2252C.java j2/C2262c.java u6/AbstractC3277j.java u6/C3267D.java u6/C3276i.java u6/K.java
00004	Get filename and put it to JSON object	file collection	Bc/l.java E7/I.java I9/a.java com/singular/sdk/internal/ApiManager.java w6/C3508c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	l9/a.java K3/j.java M1/F.java Q3/h.java U5/B.java U5/p.java V/C0928n0.java V2/i.java Y3/a.java Y3/i.java f3/d.java t3/c.java t4/C3069l.java z9/g.java
00108	Read the input stream from given URL	network command	B8/P.java B8/Y0.java S7/u.java
00016	Get location info of the device and put it to JSON object	location collection	bo/app/n.java
00015	Put buffer stream (data) to JSON object	file	u6/K.java
00078	Get the network operator name	collection telephony	H0/X.java bo/app/j0.java q3/C2835a.java u6/K.java
00171	Compare network operator with a string	network	q3/C2835a.java u6/K.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	P4/g.java S5/C0788o.java W0/n.java com/elevatelabs/geonosis/features/notifications/NotificationAlarmReceiver.java j2/C2262c.java u6/AbstractC3277j.java u6/K.java
00036	Get resource file from res/raw directory	reflection	N2/a.java S7/D.java U3/h.java W0/n.java com/elevatelabs/geonosis/features/notifications/NotificationAlarmReceiver.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/Utils.java f3/c.java o/L0.java u6/AbstractC3277j.java u6/K.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/q1.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularExceptionReporter.java com/singular/sdk/internal/SingularRequestHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	A3/e.java B8/U0.java B8/W.java B8/X0.java D6/D.java E5/C0351c.java U3/e.java com/elevatelabs/geonosis/MainActivity.java na/c.java u6/C3267D.java
00114	Create a secure socket connection to the proxy address	network command	xc/i.java
00014	Read file into a stream and put it into a JSON object	file	C6/a.java E7/I.java I7/j.java h6/k.java s6/C2978a.java z9/g.java
00012	Read data and put it into a buffer stream	file	E7/I.java U5/p.java h6/k.java o6/AbstractC2668k.java
00132	Query The ISO country code	telephony collection	G7/e.java q3/C2835a.java
00009	Put data in cursor to JSON object	file	a8/i.java com/singular/sdk/internal/OfflineEventsMigrator.java

RULE ID	BEHAVIOUR	LABEL	FILES
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	a8/i.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	a8/i.java u6/C3267D.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	a8/i.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	a8/i.java u6/C3267D.java
00189	Get the content of a SMS message	sms	u6/C3267D.java
00188	Get the address of a SMS message	sms	u6/C3267D.java
00191	Get messages in the SMS inbox	sms	com/singular/sdk/internal/DeviceInfo.java o/L0.java u6/AbstractC3277j.java u6/C3267D.java
00200	Query data from the contact list	collection contact	u6/C3267D.java
00187	Query a URI and check the result	collection sms calllog calendar	u6/C3267D.java
00201	Query data from the call log	collection calllog	u6/C3267D.java
00137	Get last known location of the device	location collection	B0/C0155e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	Bc/c.java Bc/n.java
00163	Create new Socket and connecting to it	socket	Bc/c.java Bc/n.java
00125	Check if the given file path exist	file	A3/e.java E7/I.java u6/C3276i.java
00028	Read file from assets directory	file	S7/C0810b.java
00005	Get absolute path of file and put it to JSON object	file	I9/a.java z9/g.java
00024	Write file after Base64 decoding	reflection file	C6/a.java
00147	Get the time of current location	collection location	bo/app/o.java j/p.java
00075	Get location of the device	collection location	bo/app/o.java j/p.java
00094	Connect to a URL and read data from it	command network	S7/u.java
00115	Get last known location of the device	collection location	j/p.java
00033	Query the IMEI number	collection	bo/app/j0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00083	Query the IMEI number	collection telephony	bo/app/j0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://balance-ios-ccece.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/458844225809/namespaces/firebase:fetch?key=AIzaSyABppaAA5GtXwAb0ttbBh3bRGCaCBUy3RA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'background_startup_calls': 'true', 'use_amplitude_migration': 'false'}, 'state': 'UPDATE', 'templateVersion': '16'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, 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.lab.amplitude.com	ok	**IP:** 151.101.194.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.lab.eu.amplitude.com	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
elevate-coruscant-staging.herokuapp.com	ok	**IP:** 54.205.8.205 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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:** 3.226.164.55 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gle	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
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 3.122.30.79 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
flag.lab.eu.amplitude.com	ok	**IP:** 151.101.194.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
exercises.balanceapp.com	ok	**IP:** 18.155.173.74 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
sdk-api-v1.singular.net	ok	**IP:** 23.220.73.37 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
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

DOMAIN	STATUS	GEOLOCATION
flag.lab.amplitude.com	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
exp-expanse.balanceapp.com	ok	**IP:** 104.26.9.243 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.103 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
exceptions.singular.net	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **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
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **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
coruscant.balanceapp.com	ok	**IP:** 104.26.8.243 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ana-expanse.balanceapp.com	ok	**IP:** 104.26.8.243 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 74.125.136.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
balanceapp.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
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **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
firebaseinstallations.googleapis.com	ok	**IP:** 142.250.105.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
balance-ios-ccece.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
api-diagnostics.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api2.amplitude.com	ok	**IP:** 35.161.203.136 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.131 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.balanceapp.com	ok	**IP:** 104.26.9.243 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 18.238.109.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
google.com	ok	**IP:** 142.250.9.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.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
balanceapp.com	ok	**IP:** 172.67.69.53 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c8/j.java

EMAIL	FILE
feedback@balanceapp.com	E5/C0368u.java
support@balanceapp.com	Q5/d.java
support@balanceapp.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Braze (formerly Appboy)	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/17
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
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62
Singular	Analytics	https://reports.exodus-privacy.eu.org/trackers/251

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "3d782ed233dd41e891bee4843915cda3"
"com_appboy_api_key" : "f334b94b-4f8e-445f-9930-fd828063d2cf"
"com_appboy_firebase_cloud_messaging_sender_id" : "458844225809"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"disable_all_session_ratings_cancel" : "Cancel"
"disable_all_session_ratings_disable" : "Disable"
"firebase_database_url" : "https://balance-ios-ccece.firebaseio.com"
"google_api_key" : "AIzaSyABppaAA5GtXwAb0ttbBh3bRGCaCBUy3RA"
"google_crash_reporting_api_key" : "AIzaSyABppaAA5GtXwAb0ttbBh3bRGCaCBUy3RA"
"password" : "Password"
d516587532d6684e8c9aaddbf156cf31
760ad4902b83ab7884d570c3da84dd49
c56fb7d591ba6704df047fd98f535372fea00211

POSSIBLE SECRETS
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
fa4a4428f8add91a3fedf6fabb89e548
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
kxpf4OU9IDkcp7wITcTcFgFLmSZAqMrR
37a6259cc0c1dae299a7866489dff0bd
939b6ce8acd355bebc3a889fb7cd2ec1
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
470fa2b4ae81cd56ecbcda9735803434cec591fa
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
QacvlJ8HOJpn40bmMgeWejwlPQX6RogR
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: Balance: Meditation & Sleep

Score: 4.734261 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.elevatelabs.geonosis

Developer Details: Elevate Labs, 8349798590125374140, None, https://balanceapp.com/, hello@balanceapp.com,

Release Date: May 3, 2021 **Privacy Policy:** Privacy link

Description:

Enhance your mental health, reduce daily anxiety and stress, improve your sleep, and increase focus with the Balance Meditation and Sleep app. Balance is a personalized program, like having a personal meditation coach in your pocket. You answer daily questions about your meditation experience and goals, and Balance assembles guided sessions that are perfect for you using a vast audio library of sounds, meditation music, and breathing exercises. LEARN PRACTICAL DAILY MEDITATION SKILLS Balance's meditations are organized in 10-day Plans that teach concrete meditation skills to improve your mental health and achieve your goals. You'll discover how to bring mindfulness and meditation into your daily life, increase your focus among distractions, improve your sleep, reduce anxiety, and find deep relaxation as you learn to breathe deeply to reduce anxiety and stress, accompanied by soothing white noise audio and other relaxing sounds. CALM YOUR MIND ANYTIME, ANYWHERE Balance's Singles are stand-alone guided meditations you can use anytime. Wake up gently with a morning meditation, relaxation music, or stretch with calming sounds. Then, enjoy your commute with personalized audio guidance and get to work with a library of focus music. You can breathe through animated breathing exercises to clear your mind or lower your stress, reduce anxiety, find energy, and increase your focus with quick Relax, Energize, and Concentrate daily guided meditations. No matter where you are, you can take a moment to breathe and regain balance. SLEEP WELL WITH BEDTIME RELAXATION EXERCISES Rest easy with Balance's sleep meditations, sleep stories, sleep sounds such as white noise audio, sleep music, and wind-down activities. These first-of-its-kind interactive features use bilateral stimulation and controlled breathing to help your mind relax before bed, overcome anxiety, and find more restful sleep. ENHANCE YOUR MEDITATION PRACTICE If you're a beginner, you'll start with our Foundations Plan, which trains your focus and reduces anxiety. If you already meditate often, you'll start with our Advanced Plan, which helps you take your daily meditation practice to the next level. With guided breathing exercises, you can breathe intentionally, expand your meditation skills, and build a routine that works for you. WHAT'S INCLUDED - Personalized guided meditations tailored to your mood, goals, experience, and more - 10-day Plans to help you develop and deepen your meditation skills for better mental health - Bite-sized Singles for a calming boost - Research-backed activities and calming sounds to help you relax, reduce stress and anxiety, and get restful sleep - Animated breathing exercises to help you breathe deeply and find calm - 10 concrete meditation techniques to build your practice: Breath Focus, Body Scan, and more In meditation, "one-size-fits-all" fits no one. We all have unique ways of finding relaxation, focus, rest, and happiness. Balance's audio-guided sessions help you develop mindfulness and deepen your breathing to reduce anxiety and find calm. SUBSCRIPTION DETAILS Balance offers two auto-renewing subscriptions at $11.99/month and $69.99/year. These prices are for United States customers; pricing in other countries may vary. Your subscription will automatically renew at the end of each subscription term unless auto-renewal is turned off at least 24 hours before the end of the term. Subscription renewals cost the same as the original subscription, and your credit card will be charged through your Play account at confirmation of purchase. Balance also offers a Lifetime subscription paid for by a one-off upfront payment of $399.99, which includes unlimited access to the Balance library forever. For additional information, please read our Terms of Service (http://www.balanceapp.com/balance-terms.html) and Privacy Policy (http://www.balanceapp.com/balance-privacy.html)

SCAN LOGS

Timestamp	Event	Error

2025-08-29 22:02:59	Generating Hashes	OK
2025-08-29 22:02:59	Extracting APK	OK
2025-08-29 22:02:59	Unzipping	OK
2025-08-29 22:03:00	Parsing APK with androguard	OK
2025-08-29 22:03:00	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:03:00	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:03:03	Parsing AndroidManifest.xml	OK
2025-08-29 22:03:03	Extracting Manifest Data	OK
2025-08-29 22:03:03	Manifest Analysis Started	OK
2025-08-29 22:03:03	Performing Static Analysis on: Balance (com.elevatelabs.geonosis)	OK

2025-08-29 22:03:03	Fetching Details from Play Store: com.elevatelabs.geonosis	OK
2025-08-29 22:03:04	Checking for Malware Permissions	OK
2025-08-29 22:03:04	Fetching icon path	OK
2025-08-29 22:03:04	Library Binary Analysis Started	OK
2025-08-29 22:03:04	Reading Code Signing Certificate	OK
2025-08-29 22:03:05	Running APKiD 2.1.5	OK
2025-08-29 22:03:10	Detecting Trackers	OK
2025-08-29 22:03:11	Decompiling APK to Java with JADX	OK
2025-08-29 22:03:23	Converting DEX to Smali	OK
2025-08-29 22:03:23	Code Analysis Started on - java_source	OK
2025-08-29 22:03:27	Android SBOM Analysis Completed	OK

2025-08-29 22:03:38	Android SAST Completed	OK
2025-08-29 22:03:38	Android API Analysis Started	OK
2025-08-29 22:03:48	Android API Analysis Completed	OK
2025-08-29 22:03:48	Android Permission Mapping Started	OK
2025-08-29 22:03:58	Android Permission Mapping Completed	OK
2025-08-29 22:03:58	Android Behaviour Analysis Started	OK
2025-08-29 22:04:12	Android Behaviour Analysis Completed	OK
2025-08-29 22:04:12	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:04:17	Email and URL Extraction Completed	OK
2025-08-29 22:04:17	Extracting String data from APK	OK
2025-08-29 22:04:17	Extracting String data from Code	OK

2025-08-29 22:04:17	Extracting String values and entropies from Code	OK
2025-08-29 22:04:19	Performing Malware check on extracted domains	OK
2025-08-29 22:04:22	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.