ANDROID STATIC ANALYSIS REPORT

app_icon

Cal AI (1.0.40-supperWall)

File Name:	com.viraldevelopment.calai_56.apk
Package Name:	com.viraldevelopment.calai
Scan Date:	Sept. 1, 2025, 11:12 a.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	19	1	1	1

FILE INFORMATION

File Name: com.viraldevelopment.calai_56.apk
Size: 48.43MB
MD5: 8c6bffbb139254e7324aa3663b16428f
SHA1: 82f6658f0dc884bb121955116a9d19c68ebf6882
SHA256: 1d41625e4c32bc10bc63e1a44707b940383f362ae3407f49168372b9f0a2e9e6

APP INFORMATION

App Name: Cal AI
Package Name: com.viraldevelopment.calai
Main Activity: com.calai.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.0.40-supperWall

Android Version Code: 56

APP COMPONENTS

Activities: 14
Services: 15
Receivers: 11
Providers: 4
Exported Activities: 2
Exported Services: 2
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: 2024-07-21 22:58:39+00:00
Valid To: 2054-07-21 22:58:39+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf19df3be872b2fc50efe906d067723a6652f6da7
Hash Algorithm: sha256
md5: 38279658991ac4b8e88ed198beb5be36
sha1: 25349261d60179aae52b5257c6897664f5e5a242
sha256: e59df0e1570465c2295b84755a458a02a03ff7042cfee4b4fd2093061bb5434e
sha512: b038d36acf5ca33ba5212938173245a6600a1020e59d36ca10b106c40e488a2efb0df1ec570b406176ed4ae1114337a02176a64152bd0baf61c7640cd3758ff1
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 9fe823ab8e01f3dd08a200e7f06a3a1b292e6de0338043b06cf253027975c655
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.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.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.viraldevelopment.calai.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
8c6bffbb139254e7324aa3663b16428f.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

<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
Build.HARDWARE check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes5.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
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

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.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.
4	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	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.
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: 1 | WARNING: 8 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/calai/extensions/NavigationKt.java com/calai/screens/editFavMeal/EditFavMealKt.java com/calai/screens/editMeal/EditMealKt.java com/calai/screens/main/pages/HomePageKt.java com/calai/screens/onboard/EditDailyRecommendationKt.java com/calai/screens/onboard/pages/CustomPlanViewKt.java com/calai/screens/onboard/pages/GmailLoginViewKt$GmailLoginView$4$2.java com/calai/screens/onboard/pages/GmailLoginViewKt$GmailLoginView$signUp$1.java com/calai/screens/onboard/pages/GmailLoginViewKt.java com/calai/screens/onboard/pages/RatingViewKt.java com/calai/vms/EditFavMealVM$deleteSavedFood$1$1.java com/calai/vms/EditMealDataVM.java com/calai/vms/EditMealVM$deleteSavedFood$1$1.java com/calai/vms/MainVM.java com/calai/vms/PersonalDetailVM.java com/calai/vms/SavedMealVM.java com/calai/widgets/BarCodeAnalyser.java com/calai/widgets/CameraPreviewScreenKt.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedC

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	com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/MPConfig.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/mixpanel/android/mpmetrics/MixpanelAPI.java com/mixpanel/android/mpmetrics/PersistentIdentity.java com/mixpanel/android/mpmetrics/ResourceReader.java com/mixpanel/android/mpmetrics/SessionMetadata.java com/mixpanel/android/mpmetrics/SessionReplayBroadcastReceiver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mixpanel/android/mpmetrics/SystemInformation.java com/mixpanel/android/util/HttpService.java com/mixpanel/android/util/MPLog.java com/superwall/sdk/analytics/internal/TrackingLogic.java com/superwall/sdk/billing/GoogleBillingWrapper.java com/superwall/sdk/config/ConfigLogic.java com/superwall/sdk/deprecated/PaywallMessagesKt.java com/superwall/sdk/logger/Loggable.java com/superwall/sdk/misc/CurrentActivityTracker.java com/superwall/sdk/models/serialization/AnyMapSerializer.java com/superwall/sdk/models/serialization/AnySerializer.java com/superwall/sdk/network/Network.java com/superwall/sdk/network/device/DeviceHelper.java com/superwall/sdk/network/session/CustomHttpUrlConnection.java com/superwall/sdk/paywall/presentation/rule_logic/expression_evaluator/LiquidExpressionEvaluatorParams.java com/superwall/sdk/paywall/presentation/rule_logic/javascript/NoSupportedEvaluator.java com/superwall/sdk/paywall/request/PaywallRequestManager$getPaywallResponse$2.java com/superwall/sdk/paywall/request/PaywallRequestManager$getRawPaywall$2.java com/superwall/sdk/paywall/vc/web_view/PaywallMessageKt.java com/superwall/sdk/paywall/vc/web_view/SWWebView.java com/superwall/sdk/paywall/vc/web_view/messaging/PaywallMessageHandler$didLoadWebView$3.java com/superwall/sdk/paywall/vc/web_view/messaging/PaywallMessageHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/superwall/sdk/store/transactions/TransactionManager.java com/superwall/sdk/view/SWWebViewInterface.java defpackage/TemplateLogic.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java org/threeten/bp/zone/TzdbZoneRulesCompiler.java
2	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/superwall/sdk/paywall/vc/web_view/SWWebView.java com/superwall/sdk/view/SWWebViewOld.java
3	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/superwall/sdk/view/SWWebViewOld.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/calai/retrofit/RetrofitClient.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	coil/decode/GifDecoder.java coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/calai/App.java com/calai/extensions/NavigationKt.java com/calai/google/signin/UserData.java com/mixpanel/android/util/MPConstants.java com/superwall/sdk/config/models/Survey.java com/superwall/sdk/debug/DebugViewActivity.java com/superwall/sdk/models/config/RawFeatureFlag.java com/superwall/sdk/models/triggers/TriggerRuleOccurrence.java com/superwall/sdk/paywall/vc/SuperwallPaywallActivity.java com/superwall/sdk/storage/core_data/entities/ManagedTriggerRuleOccurrence.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/PickFirstLoadBalancerProvider.java io/grpc/internal/TransportFrameUtil.java
6	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	io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/PickFirstLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	com/superwall/sdk/storage/CacheKeysKt.java
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	com/mixpanel/android/mpmetrics/MPDbAdapter.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java
10	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/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	coil/decode/SourceImageSource.java com/calai/widgets/BarCodeAnalyser.java com/calai/widgets/CameraPreviewScreenKt.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	com/calai/vms/EditMealVM.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/calai/screens/splash/SplashKt.java com/karumi/dexter/listener/SettingsClickListener.java
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java okio/Okio__JvmOkioKt.java org/threeten/bp/chrono/HijrahDate.java
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java com/github/mikephil/charting/charts/Chart.java com/superwall/sdk/storage/Storable.java
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java
00163	Create new Socket and connecting to it	socket	io/grpc/android/UdsSocket.java io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/calai/screens/splash/SplashKt.java com/karumi/dexter/listener/SettingsClickListener.java com/superwall/sdk/paywall/vc/PaywallView.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/mixpanel/android/mpmetrics/MPDbAdapter.java
00096	Connect to a URL and set request method	command network	com/mixpanel/android/util/HttpService.java com/superwall/sdk/network/Endpoint$makeRequest$2.java
00078	Get the network operator name	collection telephony	com/mixpanel/android/mpmetrics/SystemInformation.java
00089	Connect to a URL and receive input stream from the server	command network	com/mixpanel/android/util/HttpService.java
00109	Connect to a URL and get the response code	network command	com/mixpanel/android/util/HttpService.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/HttpService.java
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1066023515369/namespaces/firebase:fetch?key=AIzaSyARl_9YZoVribe03x44ZTnPchyNjLZ30fY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'active_experiment': 'none', 'force_update_current_version': '2.5.6(515)', 'force_update_current_version_android': '19', 'force_update_current_version_creator': '2.7.2(730)', 'force_update_store_url': 'https://apps.apple.com/us/app/cal-ai-calorie-tracking/id6480417616', 'paywall_remote_override': 'false', 'save_place_onboarding': 'false', 'segment': 'testLonger', 'select_daily_notification_time': 'false', 'show_live_activities': 'false', 'show_weekly_recap': 'false', 'thanksgiving_special_enabled': 'true', 'thanksgiving_swap_pages_one_two': 'true'}, 'state': 'UPDATE', 'templateVersion': '96'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_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
superwall.com	ok	**IP:** 172.67.74.93 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.apple.com	ok	**IP:** 23.32.229.38 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
api.calai.app	ok	**IP:** 216.24.57.7 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 216.58.207.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.mixpanel.com	ok	**IP:** 130.211.34.183 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
viraldevelopment.co	ok	**IP:** 76.76.21.21 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyARl_9YZoVribe03x44ZTnPchyNjLZ30fY"
"google_crash_reporting_api_key" : "AIzaSyARl_9YZoVribe03x44ZTnPchyNjLZ30fY"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426643
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

POSSIBLE SECRETS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
213b69e8e7d6cbca8efc75d14315ef1ff802d6fbc238d3cf
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
f27c2bc1a054886a5f665e0015c01056
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
11f00dc53be30cfe213781d453297cf1
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
ee4655b3ec0d2ace448aa481008538b7
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS
a0784d7a4716f3feb4f64e7f4b39bf04
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Cal AI - Food Calorie Tracker

Score: 4.6752076 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.viraldevelopment.calai

Developer Details: Improvement Tech LLC, Improvement+Tech+LLC, None, http://viraldevelopment.co, support@calai.app,

Release Date: Jul 29, 2024 **Privacy Policy:** Privacy link

Description:

CALORIE TRACKING THAT FITS A BUSY SCHEDULE Calorie counting and food logs used to be tedious until Cal AI. Just snap a photo and our smart AI calorie tracker analyzes your meal instantly. The last nutrition tracker, food tracker and macro tracker you'll ever need. Insanely accurate. Making healthy eating incredibly simple. SIMPLICITY & PRECISION IN ONE CALORIE COUNTER Other calorie counters can leave you guessing. Cal AI's calorie scanner instantly identifies your meal. Complex homemade dishes, fast food or snacks (even with packaging or directly from the bar code). Our calorie deficit calculator ensures you stay on track. Precise nutrition insights from our macro and protein tracker monitor your intake to grow muscle mass. Eliminate uncertainty and stay on a calorie deficit streak. Use our food tracker to monitor everything you eat and let the calorie calculator handle the math. That's how tracking calories works effortlessly in 2025. Whether you're following a keto diet, doing intermittent fasting, or using the macros calorie counter for bodybuilding. REAL RESULTS FROM OUR USERS: ✓ Increased body confidence and social confidence ✓ 5+ pounds lost in first week for many users ✓ Accurate AI recognition even for complex meals TAILORED FOR YOUR JOURNEY • Weight Loss: Stay motivated with our calorie deficit calculator and intuitive calorie tracking. The calorie deficit tracker ensures you stick to your diet plan and achieve your weight loss goals. Eat this much and no more. • Muscle Building: Effortlessly monitor protein, carbs and fats with our precise macro tracker and protein tracker. Add everything to your food log. • Keto Diet: Use Cal AI as a keto tracker to help you monitor carbs while staying in ketosis. The food log makes keto diet planning simple. • Intermittent Fasting: Use our food intake and meal tracker to ensure you eat healthy during your intermittent fasting eating windows. • Eat Healthier: Use Cal AI as a nutrition tracker and food journal for a healthy lifestyle. Our calories tracker keeps everything organized. ⚡ USER FAVORITE FEATURES: • Snap & Track: The food scanner captures everything in seconds. • Macro Breakdowns: Perfect your nutrition with our detailed macro calculator. • "Did I Hit My Goal?" Your calories tracker will let you know. Cheating is allowed. Just keep and eye

on your calorie deficit. • Food Memory: Your food diary remembers your frequent meals. BEFORE CAL AI VS. AFTER BEFORE: Spending 15+ minutes logging meals, guessing portions, getting frustrated AFTER: 3-second photo, accurate calorie count, and back to living your life BEFORE: Quitting your diet tracker after a week because it's too complicated AFTER: Still using Cal AI months later because it fits into your life BEFORE: Confused about whether you're eating right for your diet goals AFTER: Clear insights from your food calorie tracker and nutrition tracker YOUR TRANSFORMATION STARTS NOW Millions transformed their bodies using our food calorie tracker. Lose weight with straightforward calorie count features, gain muscle with the macro and protein tracker, stick to your diet goals with the food calculator. Take the first step today. If you have ideas or questions, please email us at support@calai.app.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 11:12:28	Generating Hashes	OK
2025-09-01 11:12:28	Extracting APK	OK
2025-09-01 11:12:28	Unzipping	OK
2025-09-01 11:12:28	Parsing APK with androguard	OK
2025-09-01 11:12:28	Extracting APK features using aapt/aapt2	OK
2025-09-01 11:12:28	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 11:12:30	Parsing AndroidManifest.xml	OK

2025-09-01 11:12:30	Extracting Manifest Data	OK
2025-09-01 11:12:30	Manifest Analysis Started	OK
2025-09-01 11:12:30	Performing Static Analysis on: Cal AI (com.viraldevelopment.calai)	OK
2025-09-01 11:12:32	Fetching Details from Play Store: com.viraldevelopment.calai	OK
2025-09-01 11:12:33	Checking for Malware Permissions	OK
2025-09-01 11:12:33	Fetching icon path	OK
2025-09-01 11:12:33	Library Binary Analysis Started	OK
2025-09-01 11:12:33	Reading Code Signing Certificate	OK
2025-09-01 11:12:34	Running APKiD 2.1.5	OK
2025-09-01 11:12:41	Detecting Trackers	OK
2025-09-01 11:12:46	Decompiling APK to Java with JADX	OK

2025-09-01 11:13:14	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 11:13:14	Decompiling classes2.dex with JADX	OK
2025-09-01 11:13:22	Decompiling classes4.dex with JADX	OK
2025-09-01 11:13:29	Decompiling classes.dex with JADX	OK
2025-09-01 11:13:38	Decompiling classes3.dex with JADX	OK
2025-09-01 11:13:46	Decompiling classes5.dex with JADX	OK
2025-09-01 11:13:54	Decompiling classes2.dex with JADX	OK
2025-09-01 11:14:03	Decompiling classes4.dex with JADX	OK
2025-09-01 11:14:09	Decompiling classes.dex with JADX	OK
2025-09-01 11:14:18	Decompiling classes3.dex with JADX	OK
2025-09-01 11:14:27	Decompiling classes5.dex with JADX	OK

2025-09-01 11:14:35	Converting DEX to Smali	OK
2025-09-01 11:14:35	Code Analysis Started on - java_source	OK
2025-09-01 11:14:38	Android SBOM Analysis Completed	OK
2025-09-01 11:14:45	Android SAST Completed	OK
2025-09-01 11:14:45	Android API Analysis Started	OK
2025-09-01 11:14:50	Android API Analysis Completed	OK
2025-09-01 11:14:50	Android Permission Mapping Started	OK
2025-09-01 11:14:55	Android Permission Mapping Completed	OK
2025-09-01 11:14:55	Android Behaviour Analysis Started	OK
2025-09-01 11:15:01	Android Behaviour Analysis Completed	OK
2025-09-01 11:15:01	Extracting Emails and URLs from Source Code	OK

2025-09-01 11:15:03	Email and URL Extraction Completed	OK
2025-09-01 11:15:03	Extracting String data from APK	OK
2025-09-01 11:15:03	Extracting String data from Code	OK
2025-09-01 11:15:03	Extracting String values and entropies from Code	OK
2025-09-01 11:15:10	Performing Malware check on extracted domains	OK
2025-09-01 11:15:11	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.