MOBSF

ANDROID STATIC ANALYSIS REPORT

MacroFactor (4.1.0)

File Name:	com.sbs.diet_517.apk
Package Name:	com.sbs.diet
Scan Date:	Sept. 1, 2025, 8:27 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	25	2	2	1

FILE INFORMATION

File Name: com.sbs.diet_517.apk
Size: 68.89MB
MD5: b8b825e27258043573192468a4913dd1
SHA1: 23eb0016a19ab40fae355daf885d12bb32533b54
SHA256: 52cb29e13a63d79a71f2a15cd55d8792835bb4e9e9077144f9dde0cdca5ace9c

APP INFORMATION

App Name: MacroFactor
Package Name: com.sbs.diet
Main Activity: com.sbs.diet.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 4.1.0

Android Version Code: 517

APP COMPONENTS

Activities: 21
Services: 21
Receivers: 23
Providers: 7
Exported Activities: 4
Exported Services: 4
Exported Receivers: 5
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: 2021-02-09 01:31:39+00:00
Valid To: 2051-02-09 01:31:39+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe60ef74e9601721e87f96566ffe8606ed48fded8
Hash Algorithm: sha256
md5: dc988091600f7ca59e8cbebfce254268
sha1: 72803ce30b7f47e84d86987f451daf8c7accb5a0
sha256: c467d82a94a851e7ab5171e3297e48e604565fa49c66a7e0deeef713bbdec234
sha512: a42288ad330167e3fe4b1d528ea9e2bf54d2db79527aff10cd1764b1f41d562b53e7acf3fa59c129edc33a74c3db422e839744f539c87eaafe8e67bc7276a392
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 60cd3a633cc441ab4a09f0282a9f24041e4d29e180e3c67034b5afc8f920b986
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.health.READ_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_NUTRITION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_NUTRITION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.READ_HYDRATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_HYDRATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

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
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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sbs.diet.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
b8b825e27258043573192468a4913dd1.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check FINDINGS: Obfuscator — DETAILS: Kiwi encrypter
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible VM check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<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.MANUFACTURER check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Obfuscator</td><td>Kiwi encrypter</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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible VM 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>classes4.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>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.sbs.diet.MainActivity	Schemes: https://, Hosts: macrofactor.page.link, link.macrofactor.app,
com.linusu.flutter_web_auth_2.CallbackActivity	Schemes: sbs://,
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: 15 | 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	Activity-Alias (com.sbs.diet.ViewPermissionUsageActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.
3	Activity (com.linusu.flutter_web_auth_2.CallbackActivity) 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
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.
5	TaskAffinity is set for activity (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [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	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	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.
11	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
12	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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.
13	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.
14	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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baseflow/permissionhandler/PermissionUtils.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	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 com/tekartik/sqflite/Constant.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/plugin/editing/SpellCheckPlugin.java io/flutter/plugins/firebase/auth/Constants.java io/flutter/plugins/firebase/crashlytics/Constants.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/imagepicker/ImagePickerCache.java io/flutter/plugins/sharedpreferences/SharedP

NO	ISSUE	SEVERITY	STANDARDS	FILES
				referencesPigeonOptions.java io/gleap/GleapWebSocketListener.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/PickFirstLoadBalancerProvider.java io/grpc/internal/TransportFrameUtil.java vn/hunghd/flutter/plugins/imagecropper/ImageCropperDelegate.java
				cachet/plugins/health/HealthPlugin$getAggregatedStepCount$1.java cachet/plugins/health/HealthPlugin$getStepsHealthConnect$1.java cachet/plugins/health/HealthPlugin$onMethodCall$1.java cachet/plugins/health/HealthPlugin.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/baseflow/googleapiavailability/GoogleApiAvailabilityManager.java com/baseflow/permissionhandler/AppSettingsManager.java com/baseflow/permissionhandler/PermissionManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/baseflow/permissionhandler/PermissionUtils.java com/baseflow/permissionhandler/ServiceManager.java com/fluttercandies/flutter_image_compress/exif/ExifKeeper.java com/fluttercandies/flutter_image_compress/ext/BitmapCompressExtKt.java com/fluttercandies/flutter_image_compress/logger/LogExtKt.java com/kineapps/flutter_file_dialog/FileDialog$copyFileToCacheDirOnBackground$1.java com/kineapps/flutter_file_dialog/FileDialog$saveFileOnBackground$1.java com/kineapps/flutter_file_dialog/FileDialog.java com/kineapps/flutter_file_dialog/FlutterFileDialogPlugin.java com/llfbandit/app_links/AppLinksHelper.java com/llfbandit/app_links/AppLinksPlugin.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java com/revenuecat/purchases_flutter/PurchasesFlutterPlugin.java com/sbs/scanner/ScannerService.java com/tekartik/sqflite/Database.java com/tekartik/sqflite/SqflitePlugin.java com/tekartik/sqflite/Utils.java com/tekartik/sqflite/dev/Debug.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java dev/britannio/in_app_review/InAppReviewPlugin.java dev/flutter/plugins/integration_test/FlutterTestRunner.java es/antonborri/home_widget/HomeWidgetBackgroundService.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/embedding/android/FlutterImageView.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/android/KeyEmbedderResponder.java io/flutter/embedding/android/KeyboardManager.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecut

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	or.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/BackGestureChannel.java io/flutter/embedding/engine/systemchannels/DeferredComponentChannel.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/systemchannels/SpellCheckChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/EventChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/ImageReaderPlatformViewRenderTarget.java io/flutter/plugin/platform/PlatformPlugin.java io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/SingleViewWindowManager.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/camera/Camera.java io/flutter/plugins/camera/CameraCaptureCallback.java io/flutter/plugins/camera/VideoRenderer.java io/flutter/plugins/camerax/InstanceManager.java io/flutter/plugins/camerax/ObserverFlutterA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				piWrapper.java io/flutter/plugins/firebase/crashlytics/FlutterFirebaseCrashlyticsPlugin.java io/flutter/plugins/firebase/firebaseremoteconfig/FirebaseRemoteConfigPlugin.java io/flutter/plugins/firebase/firestore/FlutterFirebaseFirestoreMessageCodec.java io/flutter/plugins/firebase/firestore/FlutterFirebaseFirestorePlugin.java io/flutter/plugins/firebase/firestore/utils/ExceptionConverter.java io/flutter/plugins/firebase/firestore/utils/PigeonParser.java io/flutter/plugins/firebase/messaging/ContextHolder.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/JobIntentService.java io/flutter/plugins/googlesignin/GoogleSignInPlugin.java io/flutter/plugins/imagepicker/FileUtils.java io/flutter/plugins/imagepicker/ImageResizer.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/flutter/plugins/quickactions/QuickActionsPlugin.java io/flutter/plugins/sharedpreferences/LegacySharedPreferencesPlugin.java io/flutter/plugins/sharedpreferences/SharedPreferencesPlugin.java io/flutter/plugins/urllauncher/UrlLauncherPlugin.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java
				io/gleap/Gleap.java io/gleap/GleapBanner.java io/gleap/GleapFileHelper.java io/gleap/GleapInvisibleActivityManger.java io/gleap/ScreenshotTaker.java io/gleap/SilentBugReportUtil.java io/gleap/gleap_sdk/GleapSdkPlugin.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java org/microg/safeparcel/SafeParcelUtil.java org/xmlpull/v1/XmlPullParserException.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/kineapps/flutter_file_dialog/FileDialog.java io/flutter/plugins/camera/Camera.java io/flutter/plugins/camerax/ImageCaptureHostApiImpl.java io/flutter/plugins/camerax/SystemServicesHostApiImpl.java io/gleap/HttpHelper.java org/junit/rules/TemporaryFolder.java vn/hunghd/flutter/plugins/imagecropper/FileUtils.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	com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java 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
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	com/crazecoder/openfile/utils/FileUtil.java com/yalantis/ucrop/util/FileUtils.java io/flutter/plugins/pathprovider/Messages.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/gleap/PhoneMeta.java vn/hunghd/flutter/plugins/imagecropper/FileUtils.java
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	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.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	com/tekartik/sqflite/Database.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.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	com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	io/gleap/GleapBanner.java io/gleap/GleapMainActivity.java
11	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	io/gleap/GleapBanner.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/amazon/a/a/b/b.java com/crazecoder/openfile/utils/FileUtil.java com/fluttercandies/flutter_image_compress/exif/Exif.java com/fluttercandies/flutter_image_compress/exif/ExifKeeper.java com/fluttercandies/flutter_image_compress/handle/heif/HeifHandler.java com/kineapps/flutter_file_dialog/FileDialog.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/plugins/camera/Camera.java io/flutter/plugins/camera/ImageSaver.java io/flutter/plugins/camerax/ImageCaptureHostApiImpl.java io/flutter/plugins/pathprovider/PathProviderPlugin.java
00199	Stop recording and release recording resources	record	io/flutter/plugins/camera/Camera.java
00013	Read file and put it into a stream	file	com/amazon/c/a/a/c.java com/fluttercandies/flutter_image_compress/exif/ExifKeeper.java com/kineapps/flutter_file_dialog/FileDialog.java com/revenuecat/purchases/common/FileHelper.java com/yalantis/ucrop/util/FileUtils.java io/gleap/FormDataHttpsHelper.java io/gleap/HttpHelper.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.java junit/runner/BaseTestRunner.java okio/Okio__JvmOkioKt.java org/junit/experimental/max/MaxHistory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/revenuecat/purchases/common/HTTPClient.java io/gleap/FormDataHttpsHelper.java io/gleap/GleapEventService.java io/gleap/HttpHelper.java
00089	Connect to a URL and receive input stream from the server	command network	com/revenuecat/purchases/common/HTTPClient.java io/gleap/ConfigLoader.java io/gleap/FormDataHttpsHelper.java io/gleap/GleapEventService.java io/gleap/GleapImageHandler.java io/gleap/GleapRoundImageHandler.java io/gleap/HttpHelper.java
00109	Connect to a URL and get the response code	network command	com/revenuecat/purchases/common/HTTPClient.java io/gleap/FormDataHttpsHelper.java io/gleap/GleapEventService.java io/gleap/HttpHelper.java
00092	Send broadcast	command	es/antonborri/home_widget/HomeWidgetPlugin$onMethodCall$1.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java io/gleap/FormDataHttpsHelper.java io/gleap/HttpHelper.java
00192	Get messages in the SMS inbox	sms	com/yalantis/ucrop/util/FileUtils.java vn/hunghd/flutter/plugins/imagecropper/FileUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	cachet/plugins/health/HealthPlugin.java com/amazon/a/a/i/g.java com/baseflow/permissionhandler/AppSettingsManager.java com/baseflow/permissionhandler/PermissionManager.java com/crazecoder/openfile/utils/FileUtil.java dev/britannio/in_app_review/InAppReviewPlugin.java io/flutter/plugins/urllauncher/UrlLauncher.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/FlutterImageView.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/FlutterImageView.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	cachet/plugins/health/HealthPlugin.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/baseflow/permissionhandler/AppSettingsManager.java com/baseflow/permissionhandler/PermissionManager.java com/baseflow/permissionhandler/ServiceManager.java com/linusu/flutter_web_auth_2/FlutterWebAuth2Plugin.java com/sbs/diet/enums/AppActions.java dev/britannio/in_app_review/InAppReviewPlugin.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java io/flutter/plugins/urllauncher/UrlLauncher.java io/gleap/Gleap.java io/gleap/GleapBanner.java io/gleap/GleapMainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	cachet/plugins/health/HealthPlugin.java com/baseflow/permissionhandler/AppSettingsManager.java com/baseflow/permissionhandler/PermissionManager.java com/baseflow/permissionhandler/ServiceManager.java com/sbs/diet/enums/AppActions.java io/flutter/plugins/urllauncher/UrlLauncher.java io/gleap/GleapMainActivity.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.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
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/fluttercandies/flutter_image_compress/handle/common/CommonHandler.java
00123	Save the response to JSON after connecting to the remote server	network command	io/gleap/ConfigLoader.java io/gleap/GleapEventService.java
00030	Connect to the remote server through the given URL	network	io/gleap/ConfigLoader.java io/gleap/GleapEventService.java io/gleap/GleapImageHandler.java io/gleap/GleapRoundImageHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	io/gleap/HttpHelper.java
00014	Read file into a stream and put it into a JSON object	file	io/gleap/HttpHelper.java
00072	Write HTTP input stream into a file	command network file	io/gleap/HttpHelper.java
00004	Get filename and put it to JSON object	file collection	io/gleap/HttpHelper.java io/gleap/gleap_sdk/GleapSdkPlugin.java
00153	Send binary data over HTTP	http	io/gleap/FormDataHttpsHelper.java
00094	Connect to a URL and read data from it	command network	io/gleap/FormDataHttpsHelper.java
00108	Read the input stream from given URL	network command	io/gleap/FormDataHttpsHelper.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00028	Read file from assets directory	file	io/flutter/embedding/engine/loader/ResourceExtractor.java
00202	Make a phone call	control	com/baseflow/permissionhandler/ServiceManager.java
00203	Put a phone number into an intent	control	com/baseflow/permissionhandler/ServiceManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00194	Set the audio source (MIC) and recorded file format	record	io/flutter/plugins/camera/media/MediaRecorderBuilder.java
00197	Set the audio encoder and initialize the recorder	record	io/flutter/plugins/camera/media/MediaRecorderBuilder.java
00196	Set the recorded file format and output path	record file	io/flutter/plugins/camera/media/MediaRecorderBuilder.java
00104	Check if the given path is directory	file	io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/122915645538/namespaces/firebase:fetch?key=AIzaSyDXXn2OUEq8XI8TpRL7ae38pMAOyR7FCec. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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

DOMAIN	STATUS	GEOLOCATION
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
pub.dev	ok	**IP:** 34.36.0.14 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
api-diagnostics.revenuecat.com	ok	**IP:** 35.171.209.0 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.wireless-village.org	ok	**IP:** 172.67.131.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 54.160.110.226 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
messenger-app.gleap.io	ok	**IP:** 104.26.12.7 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdk.gleap.io	ok	**IP:** 172.67.70.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
outboundmedia.gleap.io	ok	**IP:** 104.26.12.7 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.openmobilealliance.org	ok	**IP:** 172.67.75.102 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.amazon.com	ok	**IP:** 184.28.254.90 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
api.gleap.io	ok	**IP:** 67.207.79.245 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api.revenuecat.com	ok	**IP:** 54.158.163.245 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyDXXn2OUEq8XI8TpRL7ae38pMAOyR7FCec"
"google_crash_reporting_api_key" : "AIzaSyDXXn2OUEq8XI8TpRL7ae38pMAOyR7FCec"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
af60eb711bd85bc1e4d3e0a462e074eea428a8
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
36864200e0eaf5284d884a0e77d31646
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
a0784d7a4716f3feb4f64e7f4b39bf04
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: MacroFactor - Macro Tracker

Score: 4.674157 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.sbs.diet

Developer Details: Stronger By Science Technologies LLC, Stronger+By+Science+Technologies+LLC, None, https://macrofactorapp.com/, support@macrofactorapp.com,

Release Date: Sep 14, 2021 **Privacy Policy:** Privacy link

Description:

MacroFactor combines innovative coaching algorithms with proven nutrition and behavioral science to help you reach your diet goals and achieve empowering, sustainable results. MacroFactor uses a dynamic algorithm to adapt to changes in your metabolism and personalize your macro plan to keep you on track. Download to start your 7-day trial of this premium, ad-free macro tracker app. DIET SMARTER Using a best-in-class expenditure estimate, MacroFactor's nutrition coach algorithm adapts to changes in your metabolism so you never plateau. • The unique energy expenditure calculation detects changes in your metabolism • Smart algorithms personalize your calorie and macro intake targets, just like a nutrition coach would • Weekly check-ins keep you on track toward your goals The result? You better understand your body's needs and can successfully reach and sustain your goals without stress. THE BEST MACRO TRACKER TOOLS • The fastest macro tracker on the market with tools like barcode scan and custom foods • Verified food database, so you can trust the accuracy of the foods you log • Custom macro programs and weekly check-ins based on your goals and preferences • Detailed breakdowns of micronutrients, macros, and more • Period tracker, habit tracker, unique data insights and visualization, integrations, dark mode, and more AN EMPOWERING, SUSTAINABLE APPROACH MacroFactor's robust nutrition coach algorithm will make appropriate adjustments to your calorie and macro targets based on what you log, regardless of how close you came to hitting your targets from the previous week. The algorithms don't function any worse if you deviate from your macro targets. This means that unlike other nutrition coach apps, you don't have to eat like a robot or perfectly adhere to your macro targets in order to get your weekly coaching check-in and an appropriate calorie adjustment. You'll never see warnings, red numbers, or shaming when you go over your calorie or macro targets, unlike in other macro tracker apps. Instead, MacroFactor's macro tracker and nutrition coach aim to empower you with the guidance and tools you need to reach your goals without stress or rigidity. A CLOSER LOOK AT FEATURES & BENEFITS Nutrition coach • Get a science-backed macro plan designed for your goals and preferences • Set a goal to lose, maintain, or gain weight • Smart nutrition coach AI makes weekly changes to your macro plan to keep you on track Macro tracker • Large verified food database, so you can trust that calorie and macro information is accurate • Barcode scanner • Food tracker for both macros and micronutrients • Features like copy/paste, custom foods, and smart history make food tracking quick and easy • Timeline-style food log doesn't lock you in to a certain number of meals • Metric and imperial options • Custom foods and recipes Health insights tracker • Best-in-class expenditure estimate • Unique Weight Trend insight that cuts through the noise of daily fluctuations • Habit tracker • Period tracker NOTICES Contains information from Open Food Facts, which is made available here under the Open Database License (ODbL). Open Food Facts: https://openfoodfacts.org/ ODbL: https://opendatacommons.org/licenses/odbl/1-0/ SUBSCRIPTION PRICING & TERMS MacroFactor is a premium app that offers three auto-renewing subscription options: $11.99 / month $47.99 / half year $71.99 / year (equal to $5.99 a month) MacroFactor has a free trial, but does not offer a free subscription tier. These prices are for US customers. Pricing in other countries may vary. Payment will be charged to your Google Play account at confirmation of purchase. Your subscription to MacroFactor will automatically renew, unless you cancel at least 24 hours before the current period ends. You can cancel your subscription from your Google Play account settings. Terms & Conditions: https://terms.macrofactorapp.com/ Privacy Policy: https://privacy.macrofactorapp.com/

SCAN LOGS

Timestamp	Event	Error
2025-09-01 08:27:07	Generating Hashes	OK

2025-09-01 08:27:08	Extracting APK	OK
2025-09-01 08:27:08	Unzipping	OK
2025-09-01 08:27:08	Parsing APK with androguard	OK
2025-09-01 08:27:08	Extracting APK features using aapt/aapt2	OK
2025-09-01 08:27:08	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 08:27:11	Parsing AndroidManifest.xml	OK
2025-09-01 08:27:11	Extracting Manifest Data	OK
2025-09-01 08:27:11	Manifest Analysis Started	OK
2025-09-01 08:27:12	Performing Static Analysis on: MacroFactor (com.sbs.diet)	OK
2025-09-01 08:27:13	Fetching Details from Play Store: com.sbs.diet	OK
2025-09-01 08:27:15	Checking for Malware Permissions	OK

2025-09-01 08:27:15	Fetching icon path	OK
2025-09-01 08:27:15	Library Binary Analysis Started	OK
2025-09-01 08:27:15	Reading Code Signing Certificate	OK
2025-09-01 08:27:16	Running APKiD 2.1.5	OK
2025-09-01 08:27:24	Detecting Trackers	OK
2025-09-01 08:27:31	Decompiling APK to Java with JADX	OK
2025-09-01 08:27:51	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 08:27:51	Decompiling classes6.dex with JADX	OK
2025-09-01 08:27:59	Decompiling classes2.dex with JADX	OK
2025-09-01 08:28:08	Decompiling classes4.dex with JADX	OK

2025-09-01 08:28:16	Decompiling classes.dex with JADX	OK
2025-09-01 08:28:27	Decompiling classes3.dex with JADX	OK
2025-09-01 08:28:36	Decompiling classes5.dex with JADX	OK
2025-09-01 08:28:44	Decompiling classes6.dex with JADX	OK
2025-09-01 08:28:52	Decompiling classes2.dex with JADX	OK
2025-09-01 08:29:01	Decompiling classes4.dex with JADX	OK
2025-09-01 08:29:09	Decompiling classes.dex with JADX	OK
2025-09-01 08:29:19	Decompiling classes3.dex with JADX	OK
2025-09-01 08:29:28	Decompiling classes5.dex with JADX	OK
2025-09-01 08:29:36	Converting DEX to Smali	OK
2025-09-01 08:29:36	Code Analysis Started on - java_source	OK

2025-09-01 08:29:45	Android SBOM Analysis Completed	OK
2025-09-01 08:29:50	Android SAST Completed	OK
2025-09-01 08:29:50	Android API Analysis Started	OK
2025-09-01 08:29:56	Android API Analysis Completed	OK
2025-09-01 08:29:56	Android Permission Mapping Started	OK
2025-09-01 08:30:02	Android Permission Mapping Completed	OK
2025-09-01 08:30:03	Android Behaviour Analysis Started	OK
2025-09-01 08:30:09	Android Behaviour Analysis Completed	OK
2025-09-01 08:30:09	Extracting Emails and URLs from Source Code	OK
2025-09-01 08:30:12	Email and URL Extraction Completed	OK
2025-09-01 08:30:12	Extracting String data from APK	OK

2025-09-01 08:30:12	Extracting String data from Code	OK
2025-09-01 08:30:12	Extracting String values and entropies from Code	OK
2025-09-01 08:30:20	Performing Malware check on extracted domains	OK
2025-09-01 08:30:22	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.