ANDROID STATIC ANALYSIS REPORT

MealLogger (4.7.2)

File Name:	base.apk
Package Name:	com.wellnessfoundry.meallogger.android
Scan Date:	Feb. 6, 2023, 2:08 a.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	15	2	0	1

FILE INFORMATION

File Name: base.apk
Size: 9.87MB
MD5: 7a342b85ef94c77c3f9d303618822095
SHA1: e05a45cf5900eeee11ade3cd9cd4b610cd10df1e
SHA256: 9d0889dc7264100602a7081b45c14becf184501e9e7bf8b058fd26f94237e5c9

APP INFORMATION

App Name: MealLogger
Package Name: com.wellnessfoundry.meallogger.android
Main Activity: com.wellnessfoundry.meallogger.android.MainActivity
Target SDK: 26
Min SDK: 19
Max SDK:
Android Version Name: 4.7.2

Android Version Code: 571

APP COMPONENTS

Activities: 16
Services: 6
Receivers: 8
Providers: 4
Exported Activities: 0
Exported Services: 0
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=New York, L=New York, NY, O=Wellness Foundry, OU=Wellness Foundry, CN=Nicolas Wuorenheimo
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-12-13 08:55:03+00:00
Valid To: 2038-04-30 08:55:03+00:00
Issuer: C=US, ST=New York, L=New York, NY, O=Wellness Foundry, OU=Wellness Foundry, CN=Nicolas Wuorenheimo
Serial Number: 0x4d05df67
Hash Algorithm: sha1
md5: c91f7a940c8545c9422189e52e70c30a
sha1: 9fc2b6a220aa05d4d8f40f72d52cc2eb972faa63
sha256: 0afc236af130e764b6e70641a2f8a7f8c7816029fb4bc4e75d40c88ab3fdbd35
sha512: 36baa1f05566cf97faba8091f89715bf01a5c7644d4021828565c7bcecbbc022579542c34828608236a655883f7ef7fc98a56dc7e1689fe98ae76bc7b7a85275
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c5da2b2010762e316caa36af78d99f435cdb41de4d63957f50ce63f16322d267
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.wellnessfoundry.meallogger.android.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

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

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.

APKID ANALYSIS

FILE	DETAILS

<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
possible Build.SERIAL check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.wellnessfoundry.meallogger.android.MainActivity	Schemes: meallogger://, ://, Hosts: , Path Prefixes: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=19]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (com.google.android.gms.analytics.AnalyticsReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
5	Activity (com.adobe.phonegap.push.PushHandlerActivity) is Protected by a permission. Permission: com.wellnessfoundry.meallogger.android.permission.PushHandlerActivity protectionLevel: signature [android:exported=true]	info	An Activity is found to be exported, but is protected by permission.
6	Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 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.
7	Launch Mode of activity (io.intercom.android.sdk.activities.IntercomPostActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Launch Mode of activity (io.intercom.android.sdk.activities.IntercomNoteActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
9	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bolts/MeasurementEvent.java com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/GCMIntentService.java com/adobe/phonegap/push/PushDismissedHandler.java com/adobe/phonegap/push/PushHandlerActivity.java com/adobe/phonegap/push/PushPlugin.java com/adobe/phonegap/push/RegistrationIntentService.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifDecoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifencoder/AnimatedGifEncoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/MediaStoreThumbFetcher.java com/bumptech/glide/load/engine/CacheLoader.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/EngineRunnable.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/FifoPriorityThreadPoolExecutor.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ImageVideoModelLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/ImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/ImageVideoBitmapDecoder.java com/bumptech/glide/load/resource/bitmap/RecyclableBufferedInputStream.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/gif/GifResourceDecoder.java com/bumptech/glide/load/resource/gif/GifResourceEncoder.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/request/GenericRequest.java com/bumptech/glide/request/target/ViewTarget.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	com/bumptech/glide/util/ByteArrayPool.java com/bumptech/glide/util/ContentLengthInputStream.java com/desmond/squarecamera/CameraFragment.java com/desmond/squarecamera/SquareCameraPreview.java com/intercom/input/gallery/ImageCompositor.java com/plugin/datepicker/DatePickerPlugin.java io/intercom/com/bumptech/glide/Glide.java io/intercom/com/bumptech/glide/disklrucache/DiskLruCache.java io/intercom/com/bumptech/glide/gifdecoder/GifDecoder.java io/intercom/com/bumptech/glide/gifdecoder/GifHeaderParser.java io/intercom/com/bumptech/glide/gifencoder/AnimatedGifEncoder.java io/intercom/com/bumptech/glide/load/data/AssetPathFetcher.java io/intercom/com/bumptech/glide/load/data/HttpUrlFetcher.java io/intercom/com/bumptech/glide/load/data/LocalUriFetcher.java io/intercom/com/bumptech/glide/load/data/MediaStoreThumbFetcher.java io/intercom/com/bumptech/glide/load/engine/CacheLoader.java io/intercom/com/bumptech/glide/load/engine/DecodeJob.java io/intercom/com/bumptech/glide/load/engine/Engine.java io/intercom/com/bumptech/glide/load/engine/EngineRunnable.java io/intercom/com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java io/intercom/com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java io/intercom/com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java io/intercom/com/bumptech/glide/load/engine/executor/

NO	ISSUE	SEVERITY	STANDARDS	FILES
				FifoPriorityThreadPoolExecutor.java io/intercom/com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java io/intercom/com/bumptech/glide/load/model/ImageVideoModelLoader.java io/intercom/com/bumptech/glide/load/model/ResourceLoader.java io/intercom/com/bumptech/glide/load/model/StreamEncoder.java io/intercom/com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java io/intercom/com/bumptech/glide/load/resource/bitmap/Downsampler.java io/intercom/com/bumptech/glide/load/resource/bitmap/ImageHeaderParser.java io/intercom/com/bumptech/glide/load/resource/bitmap/ImageVideoBitmapDecoder.java io/intercom/com/bumptech/glide/load/resource/bitmap/RecyclableBufferedInputStream.java io/intercom/com/bumptech/glide/load/resource/bitmap/TransformationUtils.java io/intercom/com/bumptech/glide/load/resource/gif/GifResourceDecoder.java io/intercom/com/bumptech/glide/load/resource/gif/GifResourceEncoder.java io/intercom/com/bumptech/glide/manager/RequestManagerFragment.java io/intercom/com/bumptech/glide/manager/RequestManagerRetriever.java io/intercom/com/bumptech/glide/manager/SupportRequestManagerFragment.java io/intercom/com/bumptech/glide/request/GenericRequest.java io/intercom/com/bumptech/glide/request/target/ViewTarget.java io/intercom/com/bumptech/glide/util/ByteArrayPool.java io/intercom/com/bumptech/glide/util/ContentLengthInputStream.java me/leolin/shortcutbadger/ShortcutBadger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rx/internal/util/IndexedRingBuffer.java rx/internal/util/RxJavaPluginUtils.java rx/internal/util/RxRingBuffer.java
2	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/adobe/phonegap/push/GCMIntentService.java com/plugin/datepicker/DatePickerPlugin.java
3	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/desmond/squarecamera/ImageUtility.java nl/xservices/plugins/SocialSharing.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/desmond/squarecamera/BuildConfig.java
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	bolts/MeasurementEvent.java com/adobe/phonegap/push/GCMIntentService.java com/adobe/phonegap/push/PushConstants.java com/bumptech/glide/load/engine/EngineKey.java com/desmond/squarecamera/CameraFragment.java com/desmond/squarecamera/EditSavePhotoFragment.java io/intercom/com/bumptech/glide/load/engine/EngineKey.java rx/internal/schedulers/NewThreadWorker.java
6	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	bolts/WebViewAppLinkResolver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/intercom/input/gallery/ImageCompositor.java
8	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	nl/xservices/plugins/SocialSharing.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['camera', 'network connectivity'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
16	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
api.whatsapp.com	ok	**IP:** 157.240.205.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Analytics Plugin (Cordova)	Analytics	https://reports.exodus-privacy.eu.org/trackers/240
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□□<b>facebook.com/device</b>□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b&gt□□□□□□□□□□□□"

PLAYSTORE INFORMATION

Title: MealLogger-Photo Food Journal

Score: 3.34 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.wellnessfoundry.meallogger.android

Developer Details: Wellness Foundry USA, Wellness+Foundry+USA, None, http://www.meallogger.com, custserv@meallogger.com,

Release Date: Dec 18, 2010 **Privacy Policy:** Privacy link

Description:

MealLogger, the fast photo food journal, is the easy way to keep track of your healthy eating and wellness goals. Now faster and with more ways to help you stay on track. On a diet? Suffering food allergies? Managing your weight? With MealLogger you can simply photograph your food intake, add a bit of text and nutrient information if you choose, and youíre done. And, if you work with a health professional, MealLogger allows you to connect directly to your dietitian, nutritionist, fitness trainer, etc for feedback, advice, and support on your mobile device. You can get great social and one-on-one support from MealLogger, but now you can also join custom Nutrition Programs. Track your daily servings of food categories: Meats, Grains, Fish, Legumes, Vegetables, Supplements, Fruits, and more. Search for nutrition programs - like the DASH diet, or AHA guidelines. Or if you're joining MealLogger via our fitness club or health partners, you'll find programs published specifically by your club or company sponsor. Tracking servings has never been easier. Just snap a picture and tap the serving amount. No looking up food; no entering grams and calories. No more looking up one food type from hundreds of examples. And MealLogger lets you know how you're doing, meal by meal, how many more servings you need to eat that day. Connect to your friends with MealLogger groups! Create your own community based on your lifestyle, connecting with friends, family members, colleagues, or anyone sharing a common interest. If you're not yet ready to share with a group, follow a public group to learn more how others motivate each other to eat healthy or to research a specific diet you've always been curious about. Designed with privacy in mind, MealLogger groups can also be completely private -- no need to worry about posting updates to social networks or public forums where everyone can see. With private MealLogger groups, you can get same social support you love in a place built specifically for personal healthy eating conversation with those you trust. Did you know: studies show on average using a food diary can lead to a weight loss of more than 10% over the course of a year. And we all know a picture is worth a thousand words. Weíve combined the ease of photographing food, the power of social and one-on-one support with easy nutrition serving tracking. With MealLogger, weíve streamlined the process so you can also track your exercise and synch with popular trackers like Fitbit or Runkeeper in one easy-to-use app. Download your MealLogger photo food journal and begin keeping a food diary immediately. You'll be able to access your free account to save your journal to the cloud for access through multiple devices! Questions? Please contact us through the Help button on the Account page or send us an email at custserv@wellnessfoundry.com with any questions about how MealLogger can help you achieve your diet and fitness goals! If your health professional is not currently using MealLogger, contact us through the Help Button on the Account page and we will reach out to help you get connected. Take charge of your nutritional wellbeing with MealLogger, the photo food journal designed to help you eat better. Healthy eating! -The MealLogger Team

Report Generated by - MobSF v3.6.3 Beta

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.