MOBSF

ANDROID STATIC ANALYSIS REPORT

OMRON connect (7.22.0)

File Name:	com.omronhealthcare.omronconnect_609.apk
Package Name:	com.omronhealthcare.omronconnect
Scan Date:	Sept. 1, 2025, 4:16 a.m.

App Security Score: 48/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	20	0	1	1

FILE INFORMATION

File Name: com.omronhealthcare.omronconnect_609.apk
Size: 58.57MB

MD5: bc4e532e0c04ec2aabf542c9bf2c7a3f
SHA1: ce0b35bb7872765ae80c5fab0d3e66159bf90124
SHA256: eda31d112186efc54611527b79c5ec354333485345d1648b7bce86a0c2079a57

APP INFORMATION

App Name: OMRON connect
Package Name: com.omronhealthcare.omronconnect
Main Activity: com.omronhealthcare.foresight.view.module.splash.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 7.22.0
Android Version Code: 609

APP COMPONENTS

Activities: 152
Services: 16
Receivers: 22
Providers: 4
Exported Activities: 7
Exported Services: 3
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-25 00:05:03+00:00
Valid To: 2050-09-25 00:05:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6b8b158efb81ec8423909b4e82b1dc17984fed45
Hash Algorithm: sha256
md5: 8d440d03d8970c9cff9f743d2df6bcc1
sha1: 917e202e7157ffd693a39decd5af4ff4668d9b9a
sha256: 2ce0248091c485529ed5fb8dcc420f27501610a09b4a66eecde97a265333ad61
sha512: 1d117554b0a9d5d0f91ca560bf6871e67957e05eaf9a2cc39e4441f7c922b5dc32d8fb3ea46300450b0023a5b2de0fb3bcf1912138fbf7d17dbfab81faed6811
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a4b680e485b26d59535daaf6a0d2bcf93d21ab50b10abb63eeb760612f5834bb
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.omronhealthcare.omronconnect.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
com.omronhealthcare.omronconnect.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BODY_SENSORS	dangerous	grants access to body sensors, such as heart rate.	Allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: yara_issue — DETAILS: yara issue - dex file recognized by apkid but not yara module FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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>unknown (please file detection issue!)</td></tr></table>
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check SIM operator check network operator name check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.omronhealthcare.foresight.view.module.splash.SplashActivity	Schemes: omron://,
com.omronhealthcare.foresight.view.module.urlscheme.URLSchemeManagerActivity	Schemes: omron-connect://, https://, Hosts: messaging, stg-omronwellness.ohiomron.com, omronwellness.com, www.omron-healthcare.co.uk, www.omron-healthcare.com, www.omron-healthcare.de, www.omron-healthcare.it, www.omron-healthcare.es, www.omron-healthcare.be, www.omron-healthcare.bg, www.omron-healthcare.fi, www.omron-healthcare.hu, www.omron-healthcare.nl, www.omron-healthcare.pl, www.omron-healthcare.pt, www.omron-healthcare.ro, www.omron-healthcare.ch, staging.omron-healthcare.co.uk, staging.omron-healthcare.com, staging.omron-healthcare.de, staging.omron-healthcare.it, staging.omron-healthcare.es, staging.omron-healthcare.be, staging.omron-healthcare.bg, staging.omron-healthcare.fi, staging.omron-healthcare.hu, staging.omron-healthcare.nl, staging.omron-healthcare.pl, staging.omron-healthcare.pt, staging.omron-healthcare.ro, staging.omron-healthcare.ch, stg.omronconnect.eu, omronconnect.eu, staging.omron-healthcare.fr, www.omron-healthcare.fr, Paths: /subscription_promotion, /subscription_promotion/, /cardiosignal, /cardiosignal/, /oc-subscription-payment.html, Path Patterns: /.*\\omron-connect-premium.html, /.*\\omron-connect-premium2.html,
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: 1 | WARNING: 19 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Activity (com.omronhealthcare.foresight.view.module.urlscheme.URLSchemeManagerActivity) 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	Service (jp.co.omron.healthcare.communicationlibrary.ohq.OHQNotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
5	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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.
11	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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.
12	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.
13	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.
14	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.
15	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.
16	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.
17	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.
18	Activity (com.alivecor.ecg.record.AliveCorRecordLiteActivity) 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
19	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.
20	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/974237578902/namespaces/firebase:fetch?key=AIzaSyCxcJwK4N9nxZbcc-Mk70P9WL1jYkbn3tU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.READ_CALL_LOG, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	8/44	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.BLUETOOTH

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
www.alivecor.com	ok	**IP:** 34.195.109.151 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
ronhealthcaresupport@omron.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Analytics (Amazon insights)	Analytics	https://reports.exodus-privacy.eu.org/trackers/95
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"def_password" : "Password"
"google_api_key" : "AIzaSyCxcJwK4N9nxZbcc-Mk70P9WL1jYkbn3tU"
"google_crash_reporting_api_key" : "AIzaSyCxcJwK4N9nxZbcc-Mk70P9WL1jYkbn3tU"
"def_password" : "Adgangskode"
"mdtp_deleted_key" : "%1$s□□□□□□□"
"def_password" : "Passord"
"def_password" : "Passwort"
"def_password" : "Salasana"
"def_password" : "Wachtwoord"
"def_password" : "Hasło"
"def_password" : "Lozinka"
"def_password" : "Parola"
"def_password" : "Heslo"
"def_password" : "Contraseña"

POSSIBLE SECRETS
"def_password" : "Password"
"def_password" : "Palavra–passe"
"def_password" : "Jelszó"
"def_password" : "Пароль"
"def_password" : "Lösenord"
"def_password" : "Password"
"def_password" : "Password"
"def_password" : "Password"

PLAYSTORE INFORMATION

Title: OMRON connect

Score: 4.6026993 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.omronhealthcare.omronconnect

Developer Details: Omron Healthcare Inc, Omron+Healthcare+Inc, None, http://www.omronhealthcare.com, support@omronhealthcare.com,

Release Date: Jan 2, 2017 **Privacy Policy:** Privacy link

Description:

The OMRON connect app is an important part of our Going for Zero mission to eliminate heart attacks and strokes. Monitoring your blood pressure everyday can help make this vision a reality. The app makes it easy to view your health metrics anytime, anywhere. Syncing wirelessly to your smartphone or tablet, the OMRON connect app tracks your readings and daily measurements, giving you a more clear view of your overall health. Learn more at goingforzero.com The OMRON connect app provides a lot of free features for you to manage your heart health (some feature availability depends on device type) • Easily sync your readings to your smartphone via Bluetooth® • Email readings to family, physicians, or other health care professionals and share your progress • Keep track of your health history by storing and saving unlimited readings • Get a complete view of your blood pressure with systolic, diastolic and pulse readings • Receive alerts when notable changes in blood pressure are detected • Set physical activity goals and track your progress • Monitor the length and quality of your sleep • Monitor your weight and BMI (body mass index) • Access additional historical health data around sleep, weight, EKG, activity and more • Directly send readings to Google Fit In addition, the app provides the following premium features: • Gain insights into how the combination of your blood pressure, activity, sleep and weight may be affecting your heart health • Earn rewards for tracking your vitals and managing your health • Generate premium reports with more detailed information on vitals • Track medication to help rest assured that you will never miss a dose Never diagnose or treat yourself based on this system. ALWAYS consult with your physician. Note: The app will require SMS and Call Log permissions only for users of the HeartGuide™ device for messaging related notifications to work properly. The following OMRON Blood Pressure Monitors can connect to this app: Complete™ Upper Arm Blood Pressure Monitor + EKG: BP 7900 Evolv® Upper Arm: BP7000 HeartGuide™: BP8000-M, BP8000-L 10 Series Upper Arm: BP786, BP786N, BP786CAN, BP786CANN, BP7450, BP7450CAN Wrist: BP653 7 Series Upper Arm: BP761, BP761N, BP761CAN, BP761CANN, BP7350, BP7350CAN Wrist: BP654, BP6350 5 Series Upper Arm: BP7250, BP7250CAN Platinum Upper Arm: BP5450 Gold Upper Arm: BP5350 Wrist: BP4350 Silver Upper Arm: BP5250 Miscellaneous BP769CAN BP Monitor BP300 (ReliOn) The following OMRON Body Composition Monitor will connect to this app: BCM-500 For a full list of compatible devices, visit OmronHealthcare.com/connected Please visit https://s3-us-west-2.amazonaws.com/ofs-terms-production-us/OCM/en-us/eula.html to view terms of use.

SCAN LOGS

Timestamp	Event	Error

2025-09-01 04:16:32	Generating Hashes	OK
2025-09-01 04:16:32	Extracting APK	OK
2025-09-01 04:16:32	Unzipping	OK
2025-09-01 04:16:35	Parsing APK with androguard	OK
2025-09-01 04:16:37	Extracting APK features using aapt/aapt2	OK
2025-09-01 04:16:38	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 04:16:48	Parsing AndroidManifest.xml	OK
2025-09-01 04:16:48	Extracting Manifest Data	OK
2025-09-01 04:16:48	Manifest Analysis Started	OK
2025-09-01 04:16:48	Performing Static Analysis on: OMRON connect (com.omronhealthcare.omronconnect)	OK
2025-09-01 04:16:49	Fetching Details from Play Store: com.omronhealthcare.omronconnect	OK
2025-09-01 04:16:51	Checking for Malware Permissions	OK
2025-09-01 04:16:51	Fetching icon path	OK
2025-09-01 04:16:51	Library Binary Analysis Started	OK
2025-09-01 04:16:51	Reading Code Signing Certificate	OK

2025-09-01 04:16:51	Running APKiD 2.1.5	OK
2025-09-01 04:16:57	Detecting Trackers	OK
2025-09-01 04:17:01	Decompiling APK to Java with JADX	OK
2025-09-01 04:35:47	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/bc4e532e0c04ec2aabf542c9bf2c7a3f/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/bc4e532e0c04ec2aabf542c9bf2c7a3f/bc4e532e0c04ec2aabf542c9bf2c7a3f.apk'], 999.9999689757824)
2025-09-01 04:35:47	Converting DEX to Smali	OK
2025-09-01 04:35:47	Code Analysis Started on - java_source	OK
2025-09-01 04:35:47	Android SBOM Analysis Completed	OK
2025-09-01 04:35:47	Android SAST Completed	OK
2025-09-01 04:35:47	Android API Analysis Started	OK
2025-09-01 04:35:57	Android API Analysis Completed	OK
2025-09-01 05:22:22	Android Permission Mapping Started	OK
2025-09-01 05:22:25	Android Permission Mapping Completed	OK
2025-09-01 05:22:26	Android Behaviour Analysis Started	OK
2025-09-01 05:22:26	Android Behaviour Analysis Completed	OK
2025-09-01 05:22:26	Extracting Emails and URLs from Source Code	OK

2025-09-01 05:22:26	Email and URL Extraction Completed	OK
2025-09-01 05:22:26	Extracting String data from APK	OK
2025-09-01 05:22:29	Extracting String data from Code	OK
2025-09-01 05:22:29	Extracting String values and entropies from Code	OK
2025-09-01 05:22:30	Performing Malware check on extracted domains	OK
2025-09-01 05:22:37	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.