MOBSF

ANDROID STATIC ANALYSIS REPORT

Clarity (2.26.1.444)

File Name:	com.dexcom.clarity.mobile_280122601.apk
Package Name:	com.dexcom.clarity.mobile
Scan Date:	Aug. 29, 2025, 9:37 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	10	2	2	1

FILE INFORMATION

File Name: com.dexcom.clarity.mobile_280122601.apk
Size: 50.91MB
MD5: e5042642670dc31027642643a7108a73
SHA1: c5f156961322ac11077e2ac2184eac595c31dee1
SHA256: 7d43a62d5fe65874e9e63bd5b77526865eb804696cd061649af4938a15e3967f

APP INFORMATION

App Name: Clarity
Package Name: com.dexcom.clarity.mobile
Main Activity: com.dexcom.clarity.mobile.activities.Authenticate
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 2.26.1.444

Android Version Code: 280122601

APP COMPONENTS

Activities: 5
Services: 12
Receivers: 12
Providers: 4
Exported Activities: 0
Exported Services: 1
Exported Receivers: 3
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=CA, L=San Diego, O=Dexcom, OU=Research and Development, CN=Android Development Team
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-09-25 15:38:39+00:00
Valid To: 2040-09-18 15:38:39+00:00
Issuer: C=US, ST=CA, L=San Diego, O=Dexcom, OU=Research and Development, CN=Android Development Team
Serial Number: 0x1a7999a7
Hash Algorithm: sha256
md5: f81482a82de6c68428c0cd55f91b72f5
sha1: 050f7b7bdc16dd198c2770d69182ceddbc443184
sha256: 2c5aa799006136a39e7ca2d6d3460856e51470e52ea21c0535ab0c127f2a4da6
sha512: a3a1b5b67eb969a172849ca348c67fb1500e4c1332ab75ae6d85e763354f1329f7eb2be9bb1bc275bdf66feb2639f0520fc7062bec876785f19ff467962d9734
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3b599f658e7b26142073b3521f46e84157de2a478494ce8939d050dccd181836
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.dexcom.g6.content_provider.READ_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.dexcom.cgm.content_provider.READ_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.dexcom.clarity.firebase.READ_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.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.dexcom.clarity.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
e5042642670dc31027642643a7108a73.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>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>
<tr><td>classes2.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>
<tr><td>classes3.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>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
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>

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: 5 | 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	Service (qk.EQj) is Protected by a permission. Permission: com.dexcom.clarity.firebase.READ_PERMISSION protectionLevel: signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.
3	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.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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: 3 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	qk/C0563Jkj.java qk/C0900Poj.java qk/C1015Rkj.java qk/C1415Ykj.java qk/C2476iZj.java qk/C2598jZK.java qk/C3246pDj.java qk/C3423qZK.java qk/C3719tFj.java qk/KZK.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	qk/C0510ImK.java qk/C2763kmK.java qk/C4158wkK.java qk/C4296xmK.java
3	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/datadog/android/ndk/internal/NdkCrashLog.java com/datadog/opentracing/DDTraceOTInfo.java com/datadog/trace/api/DDTraceApiInfo.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/datadog/android/trace/AndroidTracer.java com/datadog/opentracing/DDTracer.java com/datadog/opentracing/StringCachingBigInteger.java qk/C1516ZxK.java qk/C2269gmK.java qk/C2957mSj.java qk/C3395qPK.java qk/C4209xG.java qk/C4472zAK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	qk/C0113BdK.java qk/IQj.java
6	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	qk/C0388Gij.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	qk/C4248xU.java
00162	Create InetSocketAddress object and connecting to it	socket	qk/C0744MmK.java qk/C4158wkK.java
00163	Create new Socket and connecting to it	socket	qk/C0744MmK.java qk/C4158wkK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	com/dexcom/clarity/mobile/Components.java com/dexcom/dxoauthlibrary/OAuthConnectionSettings.java qk/LQ.java
00022	Open a file from given absolute path of the file	file	com/datadog/android/core/internal/persistence/BatchId.java com/datadog/android/ndk/internal/DatadogNdkCrashHandler.java qk/C1247VsK.java qk/JZ.java qk/XY.java qk/YQj.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	qk/VSj.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	qk/C3246pDj.java qk/VSj.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/dexcom/clarity/mobile/main/MainActivityVm.java qk/C3246pDj.java qk/NDj.java qk/RPj.java qk/WAK.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/dexcom/clarity/mobile/main/MainActivityVm.java qk/RPj.java qk/WAK.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	qk/C3246pDj.java
00187	Query a URI and check the result	collection sms calllog calendar	qk/C3036nGj.java qk/C3246pDj.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	qk/C3246pDj.java
00109	Connect to a URL and get the response code	network command	qk/C2740ke.java qk/C4592zqj.java qk/RunnableC2102fOj.java qk/RunnableC4394yWj.java qk/VRj.java
00091	Retrieve data from broadcast	collection	com/datadog/android/rum/tracking/ActivityLifecycleTrackingStrategy.java
00089	Connect to a URL and receive input stream from the server	command network	qk/C2740ke.java qk/RunnableC2102fOj.java qk/RunnableC4394yWj.java qk/VRj.java
00094	Connect to a URL and read data from it	command network	qk/C2740ke.java qk/RunnableC2102fOj.java qk/RunnableC4394yWj.java
00108	Read the input stream from given URL	network command	qk/C2740ke.java qk/RunnableC2102fOj.java qk/RunnableC4394yWj.java
00013	Read file and put it into a stream	file	com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java qk/C0532IxK.java qk/C3509rGj.java qk/ZF.java
00030	Connect to the remote server through the given URL	network	qk/RunnableC2102fOj.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	qk/C2740ke.java qk/VRj.java
00015	Put buffer stream (data) to JSON object	file	qk/C2740ke.java
00012	Read data and put it into a buffer stream	file	com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java
00112	Get the date of the calendar event	collection calendar	qk/TIK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://clarity-mobile-production.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/640912650727/namespaces/firebase:fetch?key=AIzaSyC8p_fylW_cgCWs2TUAIRI9r6yAGXumXWQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
clarity-mobile-production.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.dexcom.com	ok	**IP:** 162.159.130.80 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u000eu8ge@e5.bl9bq4	qk/C2426iEK.java
1.@0.h0	qk/WJ.java
u0004r4jhng@ej.60 u001bhfga@rhoou.xn	com/datadog/android/okhttp/trace/TracingInterceptor.java
y@sӳ.x5	com/datadog/android/rum/model/ViewEvent.java

EMAIL	FILE
qum@pmcwa.sqeg	com/datadog/android/rum/internal/domain/scope/RumRawEvent.java

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
"auth_authenticating" : "Authenticating"
"firebase_database_url" : "https://clarity-mobile-production.firebaseio.com"
"google_api_key" : "AIzaSyC8p_fylW_cgCWs2TUAIRI9r6yAGXumXWQ"
"google_crash_reporting_api_key" : "AIzaSyC8p_fylW_cgCWs2TUAIRI9r6yAGXumXWQ"
"pref_best_day_key" : "pref_best_day"
"pref_env_vals_key" : "pref_env_vals"

POSSIBLE SECRETS
"pref_goal_time_in_range_key" : "pref_goal_time_in_range"
"pref_patterns_key" : "pref_patterns"
"pref_time_in_range_key" : "pref_time_in_range"
"pref_weekly_report_key" : "pref_weekly_report"
"pref_weekly_report_pre_accept_key" : "pref_weekly_pre_accept_report"
"preference_file_key" : "com.dexcom.clarity"
"wnf_user_email_token" : "user_email"

PLAYSTORE INFORMATION

Title: Dexcom Clarity

Score: 3.9512196 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.dexcom.clarity.mobile

Developer Details: Dexcom, Dexcom, None, http://www.dexcom.com/customer-care/contact-us, appsupport@dexcom.com,

Release Date: Aug 5, 2017 **Privacy Policy:** Privacy link

Description:

Dexcom Clarity is a diabetes management application for CGM users. It provides relevant insights into users' retrospective glucose values, patterns, and trends over time. Dexcom Clarity is an important part of your Dexcom CGM system. It can help you identify glucose patterns and, with your healthcare professional, determine the potential causes of those patterns. Dexcom Clarity users experience up to 15% increased time in range (70-180mg/dL) as compared to non-users.* Log in with your Dexcom account to: • Keep tabs on your time in range, patterns and other key metrics. • Allow clinics to access to your data and reports to make appointments more efficient. • Set Time in Range goals. • Turn on daily or weekly notifications and emails. • View, save, print, and email all reports. • Connect to partner apps for more features and benefits. This app store should not be used as your first point of contact to resolve technical or customer services issues. In order to protect your privacy and personal information, and promptly resolve any technical or customer services issues you are having with any Dexcom product, please contact 1-888-738-3646. Dexcom

is required to follow up with customers regarding product-related complaints. If Dexcom determines that your comment/complaint requires follow up, a technical support representative will attempt to contact you to gather more information regarding your comment/complaint. *Parker AS, Welsh J, Jimenez A, Walker T. Insights from big data (2): Benefits of self-guided retrospective review of continuous glucose monitoring reports. Diabetes Technol Ther. 2018;20(S1):A-27.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:37:23	Generating Hashes	OK
2025-08-29 21:37:23	Extracting APK	OK
2025-08-29 21:37:23	Unzipping	OK
2025-08-29 21:37:23	Parsing APK with androguard	OK
2025-08-29 21:37:23	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:37:23	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:37:25	Parsing AndroidManifest.xml	OK
2025-08-29 21:37:25	Extracting Manifest Data	OK

2025-08-29 21:37:25	Manifest Analysis Started	OK
2025-08-29 21:37:25	Performing Static Analysis on: Clarity (com.dexcom.clarity.mobile)	OK
2025-08-29 21:37:26	Fetching Details from Play Store: com.dexcom.clarity.mobile	OK
2025-08-29 21:37:26	Checking for Malware Permissions	OK
2025-08-29 21:37:26	Fetching icon path	OK
2025-08-29 21:37:26	Library Binary Analysis Started	OK
2025-08-29 21:37:26	Reading Code Signing Certificate	OK
2025-08-29 21:37:27	Running APKiD 2.1.5	OK
2025-08-29 21:37:30	Detecting Trackers	OK
2025-08-29 21:37:34	Decompiling APK to Java with JADX	OK
2025-08-29 21:38:08	Converting DEX to Smali	OK

2025-08-29 21:38:09	Code Analysis Started on - java_source	OK
2025-08-29 21:38:12	Android SBOM Analysis Completed	OK
2025-08-29 21:38:21	Android SAST Completed	OK
2025-08-29 21:38:21	Android API Analysis Started	OK
2025-08-29 21:38:29	Android API Analysis Completed	OK
2025-08-29 21:38:29	Android Permission Mapping Started	OK
2025-08-29 21:38:36	Android Permission Mapping Completed	OK
2025-08-29 21:38:36	Android Behaviour Analysis Started	OK
2025-08-29 21:38:46	Android Behaviour Analysis Completed	OK
2025-08-29 21:38:46	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:38:51	Email and URL Extraction Completed	OK

2025-08-29 21:38:51	Extracting String data from APK	OK
2025-08-29 21:38:52	Extracting String data from Code	OK
2025-08-29 21:38:52	Extracting String values and entropies from Code	OK
2025-08-29 21:38:59	Performing Malware check on extracted domains	OK
2025-08-29 21:39:00	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.