MOBSF

ANDROID STATIC ANALYSIS REPORT

LiveHealth (20.01.040)

File Name:	com.americanwell.android.member.wellpoint_200100012.apk
Package Name:	com.americanwell.android.member.wellpoint
Scan Date:	Aug. 29, 2025, 7:37 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	17	3	2	1

FILE INFORMATION

File Name: com.americanwell.android.member.wellpoint_200100012.apk
Size: 6.56MB
MD5: 3dd9bf8ae4014f2a331965578fe09bac
SHA1: df40f02a4b586312e620343db7fc0b6d587b09f4
SHA256: a655a3a4fb50bfc8fb94ead29c8251e9016f5aaf2d289275b594a736f2f86dd6

APP INFORMATION

App Name: LiveHealth
Package Name: com.americanwell.android.member.wellpoint
Main Activity: com.americanwell.android.member.wellpoint.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 20.01.040

Android Version Code: 200100012

APP COMPONENTS

Activities: 12
Services: 6
Receivers: 4
Providers: 4
Exported Activities: 4
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Boston, O=AmericanWell, OU=Development, CN=Online Care
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-08-09 15:24:16+00:00
Valid To: 2040-12-25 15:24:16+00:00
Issuer: C=US, ST=MA, L=Boston, O=AmericanWell, OU=Development, CN=Online Care
Serial Number: 0x520509a0
Hash Algorithm: sha1
md5: 8ba1e42dddc467c33487ff1037266ca3
sha1: f2d0db5c706156804ef9c6ff928d82332e192805
sha256: 3c8e68d75c5949a88b42a84eb6a358677fc47eaaf547e972128f409a620c2954
sha512: a1e1196f579ed5b66b7b0a62afbe1516a45b5549e96519f34220a630e96b71529bca862a95fa4670ce2bd8c405c406b72ec798ba5733cd45232879958d5ed14b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a2a266be03da5ca7e26ba291eaa0ddf6c5d769178d394f338fdade9e79d79cd8
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.americanwell.android.member.wellpoint.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<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 Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible ro.secure check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.americanwell.android.member.wellpoint.MainActivity	Schemes: https://, Hosts: converge.livehealthonline.com, patient-link-app.cvg01.amwell.systems, amg-consumer-client.cvg01.amwell.systems, Path Prefixes: /auth0, Path Patterns: /DIRECT/default/messages.*, ..*/WLPT/authType/DIRECT.*,
com.auth0.android.provider.RedirectActivity	Schemes: test://, awwellpoint://, Hosts: test-domain, login.converge.amwell.com, Path Prefixes: /android/com.americanwell.android.member.wellpoint/callback,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.auth0.android.provider.RedirectActivity) 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 (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.
5	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	pa/a.java xe/c.java xe/d.java xe/i.java xe/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/c1.java bo/app/c6.java bo/app/e.java bo/app/f4.java bo/app/f6.java bo/app/h1.java bo/app/i0.java bo/app/j0.java bo/app/j3.java bo/app/k0.java bo/app/l6.java bo/app/m.java bo/app/r0.java bo/app/u5.java bo/app/v0.java bo/app/w4.java bo/app/z.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java l1/k.java
3	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/d.java io/flutter/plugin/platform/g.java
				a2/b.java a4/a.java a5/f.java a5/n.java b4/a.java b7/c.java b7/d.java b8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/d.java c1/f.java c1/m.java c2/a.java c2/q.java c2/s.java c2/u.java com/auth0/android/provider/a.java com/auth0/android/provider/c.java com/auth0/android/provider/e.java com/auth0/android/provider/h.java com/auth0/android/provider/l.java com/auth0/android/provider/m.java com/auth0/android/provider/q.java com/auth0/android/request/internal/a.java com/auth0/android/request/internal/l.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/b.java com/baseflow/geolocator/j.java com/baseflow/geolocator/m.java com/braze/support/BrazeLogger.java com/newrelic/agent/android/ndk/AgentNDK.java d4/l.java d4/m.java d4/n.java f3/b.java f3/b0.java f3/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	f3/c0.java f3/j.java f3/v.java f3/w.java f3/y.java f6/a.java f6/e.java f8/b.java g3/c.java g3/k.java g3/o.java g6/h.java h1/a.java h6/a.java h6/b.java ha/a.java i0/a.java i0/b.java i0/b1.java i0/d0.java i0/f.java i0/k0.java i0/n0.java i0/p.java i0/q0.java i0/r.java i0/r0.java i0/u0.java i0/v0.java i0/y0.java i6/b.java i6/d.java io/flutter/plugins/webviewflutter/f.java io/flutter/plugins/webviewflutter/o3.java j0/d.java j3/e0.java j3/k0.java j3/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j3/x.java k/e.java k/i.java k/k.java k/m.java k/n.java k/q.java k/r.java k1/b.java l1/e.java l1/j.java m/a.java m/b.java n9/i.java o3/b.java o4/a.java o4/b.java o4/c.java o5/b.java o9/a.java o9/d0.java p3/m.java p5/c.java p9/i.java pe/d.java r/d.java s2/k.java t/g.java t0/a.java v2/a.java w/d.java w8/m.java w8/r.java w8/w1.java x4/e.java ye/c.java z0/a.java z0/e.java z1/j.java z6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	fa/a.java fa/c.java fa/d.java fa/e.java y6/h.java z2/m0.java z2/t0.java
6	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	a8/a.java
7	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	bo/app/b1.java com/braze/support/IntentUtils.java m7/q.java nb/a.java nb/b.java ob/a.java
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/braze/support/StringUtils.java
9	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	i6/b.java i6/d.java j6/e.java n9/a.java n9/i.java o2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	bo/app/u4.java com/braze/configuration/BrazeConfig.java o9/c0.java v6/n.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	a8/b.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	g6/h.java k/n.java
13	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	i6/d.java o5/c.java w8/m.java
14	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	e8/b.java o5/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	a0/m.java b7/g.java b7/r.java bo/app/u5.java com/braze/Braze.java com/braze/images/DefaultBrazeImageLoader.java com/braze/support/BrazeFileUtils.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/newrelic/agent/android/ndk/AgentNDK.java com/newrelic/agent/android/ndk/ManagedContext.java i6/d.java i8/d.java m7/i.java n9/i.java o2/a.java w8/m.java w8/m0.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	b2/a.java c2/a.java c2/q.java c2/u.java com/auth0/android/provider/d.java com/auth0/android/provider/q.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java d4/n.java e6/a.java i6/b.java p9/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00023	Start another application from current application	reflection control	e6/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	b2/a.java c2/a.java c2/q.java c2/u.java e6/a.java p9/h.java
00078	Get the network operator name	collection telephony	bo/app/j0.java ca/a.java m7/c.java
00013	Read file and put it into a stream	file	a0/m.java bo/app/l0.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java hb/j.java i6/d.java ka/a.java m7/o.java o5/c.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/m1.java
00036	Get resource file from res/raw directory	reflection	b2/a.java c2/a.java c2/q.java com/auth0/android/provider/q.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java o2/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00026	Method reflection	reflection	fc/a.java fc/b.java
00202	Make a phone call	control	c2/u.java
00203	Put a phone number into an intent	control	c2/u.java
00096	Connect to a URL and set request method	command network	m6/c.java p5/c.java v6/o.java
00089	Connect to a URL and receive input stream from the server	command network	p5/c.java v6/o.java
00109	Connect to a URL and get the response code	network command	m6/c.java p5/c.java ra/b.java t6/c.java v6/o.java
00194	Set the audio source (MIC) and recorded file format	record	j9/f.java
00197	Set the audio encoder and initialize the recorder	record	j9/f.java
00196	Set the recorded file format and output path	record file	j9/f.java
00199	Stop recording and release recording resources	record	w8/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	h7/f.java v6/o.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/e.java t/g.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java t/g.java
00091	Retrieve data from broadcast	collection	com/braze/push/BrazeNotificationUtils.java
00114	Create a secure socket connection to the proxy address	network command	te/f.java
00162	Create InetSocketAddress object and connecting to it	socket	m7/k.java xe/b.java xe/j.java
00163	Create new Socket and connecting to it	socket	m7/k.java xe/b.java xe/j.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/l.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/l.java
00012	Read data and put it into a buffer stream	file	i6/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	o5/c.java
00094	Connect to a URL and read data from it	command network	v6/o.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK
Other Common Permissions	2/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE

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
c.us.heap-api.com	ok	**IP:** 44.216.142.23 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
auth0.com	ok	**IP:** 104.18.37.18 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
manage.auth0.com	ok	**IP:** 172.64.148.184 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.58 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	g3/j.java

TRACKERS

TRACKER	CATEGORIES	URL
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130

HARDCODED SECRETS

POSSIBLE SECRETS
"com_braze_api_key" : "95e9e26e-ae7f-4aef-a444-00e3e0421f9d"
"com_braze_firebase_cloud_messaging_sender_id" : "584450777417"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"

POSSIBLE SECRETS
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
d47a8bfb-8e56-4fac-8051-0632b1f2b74c
389C9738-A761-44DE-8A66-1668CFD67DA1
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
37a6259cc0c1dae299a7866489dff0bd
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg

PLAYSTORE INFORMATION

Title: LiveHealth Online Mobile

Score: 3.976155 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.americanwell.android.member.wellpoint

Developer Details: American Well Corporation, American+Well+Corporation, None, http://www.livehealthonline.com, help@livehealthonline.com,

Release Date: Oct 9, 2013 **Privacy Policy:** Privacy link

Description:

Speak with board-certified doctors, licensed therapists, psychiatrists and more through live video on your smartphone, tablet, or computer. LiveHealth Online is an easy and convenient way to get the care you need whether you’re at home, at work, or on the go! Download the app and sign up to get started. 24/7 virtual urgent care with board-certified doctors for the whole family. Counselling and talk therapy with licensed therapists. Scheduled consultations with psychiatrists. Primary care, dermatologists, dieticians, lactation consultations and other benefits may be available depending on your health insurance.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:37:12	Generating Hashes	OK
2025-08-29 19:37:12	Extracting APK	OK
2025-08-29 19:37:12	Unzipping	OK
2025-08-29 19:37:12	Parsing APK with androguard	OK
2025-08-29 19:37:13	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:37:13	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:37:14	Parsing AndroidManifest.xml	OK
2025-08-29 19:37:14	Extracting Manifest Data	OK
2025-08-29 19:37:14	Manifest Analysis Started	OK

2025-08-29 19:37:15	Performing Static Analysis on: LiveHealth (com.americanwell.android.member.wellpoint)	OK
2025-08-29 19:37:16	Fetching Details from Play Store: com.americanwell.android.member.wellpoint	OK
2025-08-29 19:37:16	Checking for Malware Permissions	OK
2025-08-29 19:37:16	Fetching icon path	OK
2025-08-29 19:37:16	Library Binary Analysis Started	OK
2025-08-29 19:37:16	Reading Code Signing Certificate	OK
2025-08-29 19:37:17	Running APKiD 2.1.5	OK
2025-08-29 19:37:19	Detecting Trackers	OK
2025-08-29 19:37:20	Decompiling APK to Java with JADX	OK
2025-08-29 19:37:29	Converting DEX to Smali	OK
2025-08-29 19:37:30	Code Analysis Started on - java_source	OK

2025-08-29 19:37:31	Android SBOM Analysis Completed	OK
2025-08-29 19:37:37	Android SAST Completed	OK
2025-08-29 19:37:37	Android API Analysis Started	OK
2025-08-29 19:37:43	Android API Analysis Completed	OK
2025-08-29 19:37:43	Android Permission Mapping Started	OK
2025-08-29 19:37:48	Android Permission Mapping Completed	OK
2025-08-29 19:37:48	Android Behaviour Analysis Started	OK
2025-08-29 19:37:55	Android Behaviour Analysis Completed	OK
2025-08-29 19:37:55	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:37:57	Email and URL Extraction Completed	OK
2025-08-29 19:37:57	Extracting String data from APK	OK

2025-08-29 19:37:57	Extracting String data from Code	OK
2025-08-29 19:37:57	Extracting String values and entropies from Code	OK
2025-08-29 19:37:58	Performing Malware check on extracted domains	OK
2025-08-29 19:38:02	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.