MOBSF

ANDROID STATIC ANALYSIS REPORT

Amwell (13.05.00.000)

File Name:	com.americanwell.android.member.amwell_130500000.apk
Package Name:	com.americanwell.android.member.amwell
Scan Date:	Aug. 29, 2025, 7:36 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	11	3	2	2

FILE INFORMATION

File Name: com.americanwell.android.member.amwell_130500000.apk
Size: 25.56MB
MD5: 30d8e860b126e79fea2e9d905f1b95e1
SHA1: 44ebd5f765e148ba3090dbf30d844a207892d05d
SHA256: 3038e0a0f048824983829a71b57458fd2415a236846728a8af204cde8cae9ea2

APP INFORMATION

App Name: Amwell
Package Name: com.americanwell.android.member.amwell
Main Activity: com.americanwell.android.member.activity.StartActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 13.05.00.000

Android Version Code: 130500000

APP COMPONENTS

Activities: 125
Services: 4
Receivers: 2
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
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.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.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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.

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.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.facebook.katana.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check
	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.americanwell.android.member.activity.StartActivity	Schemes: amwell://, Hosts: americanwell.com,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

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

HIGH: 1 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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.
3	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) 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.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/a/a/a/e.java c/a/a/a/f.java c/b/a/a/c.java c/b/a/a/e.java c/b/a/a/h.java c/b/a/a/i.java c/c/a/a/b/k.java c/c/a/a/d/a.java c/f/a/g0.java com/americanwell/android/member/activity/AccessiblityModeActivity.java com/americanwell/android/member/activity/EnterPasscodeActivity.java com/americanwell/android/member/activity/LoginActivity.java com/americanwell/android/member/activity/SplashActivity.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/americanwell/android/member/activity/TwoFactorAuthenticationActivity.java com/americanwell/android/member/activity/TwoFactorAuthenticationValidationActivity.java com/americanwell/android/member/activity/engagement/CostCheckBeforeEngagementActivity.java com/americanwell/android/member/activity/engagement/MatchmakerActivity.java com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java com/americanwell/android/member/activity/engagement/StartVisitActivity.java com/americanwell/android/member/activity/menudrawer/AbsActionableMenuDrawerItem.java com/americanwell/android/member/activity/menudrawer/AbsMenuDrawerActivity.java com/americanwell/android/member/activity/menudrawer/AbsSimpleTextMenuDrawerItem.java com/americanwell/android/member/activity/menudrawer/ActivityMenuDrawerItem.java com/americanwell/android/member/activity/menudrawer/MethodMenuDrawerItem.java com/americanwell/android/member/activity/messages/AbsMessageRelatedActivity.java com/americanwell/android/member/activity/participant/JoinVideoConferenceActivity.java com/americanwell/android/member/activity/participant/WaitingRoomActivity.java com/americanwell/android/member/activity/providers/SpeedPassActivity.java com/americanwell/android/member/activity/settings/MyPreferencesActivity.java com/americanwell/android/member/activity/settings/SettingsActivity.java com/americanwell/android/member/activity/setup/ExperienceImprovedMobileEnrolledActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/americanwell/android/member/fragment/AWCameraFragment.java com/americanwell/android/member/fragment/FindActiveVisitsResponderFragment.java com/americanwell/android/member/fragment/MatchmakerCreateRequestResponderFragment.java com/americanwell/android/member/fragment/MemberEmailAvailableResponderFragment.java com/americanwell/android/member/util/PDFTools.java com/americanwell/sdk/internal/visitconsole/view/g.java com/braze/support/BrazeLogger.java g/i0/b.java g/i0/j/i/c.java
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/b0.java bo/app/d6.java bo/app/e.java bo/app/f1.java bo/app/g6.java bo/app/h4.java bo/app/l0.java bo/app/l1.java bo/app/m.java bo/app/m0.java bo/app/m6.java bo/app/n0.java bo/app/r3.java bo/app/v5.java bo/app/w4.java bo/app/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java
				bo/app/u4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/americanwell/android/member/activity/LoginActivity.java com/americanwell/android/member/activity/engagement/MatchmakerActivity.java com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java com/americanwell/android/member/activity/engagement/ReviewInsuranceActivity.java com/americanwell/android/member/activity/providers/SpeedPassActivity.java com/americanwell/android/member/activity/setup/CompleteEnrollmentActivity.java com/americanwell/android/member/activity/setup/ExperienceImprovedMobileEnrolledActivity.java com/americanwell/android/member/activity/setup/TellUsAboutYourselfActivity.java com/americanwell/android/member/entities/provider/info/Language.java com/americanwell/android/member/fragment/AuthenticateMemberResponderFragment.java com/americanwell/android/member/fragment/CompleteEnrollmentResponderFragment.java com/americanwell/android/member/fragment/CreateSpeedPassEngagementResponderFragment.java com/americanwell/android/member/fragment/CreateTransferVidyoEngagementFragment.java com/americanwell/android/member/fragment/DependentHealthSummaryResponderFragment.java com/americanwell/android/member/fragment/EditAccountResponderFragment.java com/americanwell/android/member/fragment/GetAccountInfoResponderFragment.java com/americanwell/android/member/fragment/HealthSummaryResponderFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/americanwell/android/member/fragment/MemberEmailAvailableResponderFragment.java com/americanwell/android/member/fragment/SendMessageInfoResponderFragment.java com/americanwell/android/member/fragment/SendPairingCodeResponderFragment.java com/americanwell/android/member/fragment/ShareExamDataResponderFragment.java com/americanwell/android/member/fragment/UpdateGroupKeyResponderFragment.java com/americanwell/android/member/fragment/UpdateMemberAuthenticationResponderFragment.java com/americanwell/android/member/fragment/UpgradeMemberAuthenticationResponderFragment.java com/americanwell/android/member/fragment/ValidatePairingCodeResponderFragment.java com/americanwell/android/member/fragment/VideoMetricsResponderFragment.java com/americanwell/android/member/fragment/VidyoEngagementResponderFragment.java com/americanwell/android/member/fragment/VidyoEngagementUpdateResponderFragment.java com/americanwell/android/member/location/FetchAddressIntentService.java com/americanwell/android/member/restws/RestClientService.java com/americanwell/android/member/tracking/MatomoTracker.java com/americanwell/android/member/tracking/PropertiesInfoButtonDescription.java com/americanwell/android/member/util/BiometricLoginHelper.java com/americanwell/android/member/util/Constants.java com/americanwell/sdk/entity/SDKErrorReaso

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n.java com/americanwell/sdk/entity/SDKSuggestion.java com/americanwell/sdk/internal/AWSDKImpl.java com/americanwell/sdk/manager/ValidationConstants.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/braze/configuration/BrazeConfig.java g/i0/j/c.java g/i0/j/d.java g/i0/j/g.java g/i0/j/h.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	c/b/a/a/h.java com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java com/americanwell/android/member/util/PDFTools.java
6	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 i/a/a/h/b.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/e1.java com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java com/americanwell/android/member/activity/participant/WaitingRoomActivity.java com/braze/support/IntentUtils.java e/c0/a.java e/c0/b.java e/c0/d/a.java i/a/a/e.java
8	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	com/americanwell/android/member/util/Utils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	com/americanwell/android/member/util/BiometricLoginHelper.java
10	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/americanwell/android/member/activity/chat/AIChatFragment.java com/americanwell/android/member/activity/consumerHome/ConsumerHomeWebViewFragment.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/americanwell/android/member/amwell/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	com/americanwell/android/member/activity/dependent/EditDependentActivity.java com/americanwell/android/member/activity/healthplan/HealthPlanFragment.java com/americanwell/android/member/util/Utils.java com/americanwell/sdk/entity/SDKLocalDate.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/americanwell/android/member/activity/BaseManagePermissionsActivity.java com/americanwell/android/member/activity/LoginActivity.java com/americanwell/android/member/activity/SplashActivity.java com/americanwell/android/member/activity/WebViewActivity.java com/americanwell/android/member/activity/consumerHome/ConsumerHomeActivity.java com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java com/americanwell/android/member/activity/engagement/StartVisitActivity.java com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java com/americanwell/android/member/activity/engagement/tytoLiveStream/TytoLiveStreamQRStatusFragment.java com/americanwell/android/member/activity/settings/AboutActivity.java com/americanwell/android/member/activity/settings/ContactActivity.java com/americanwell/android/member/activity/setup/AccessNotEnabledActivity.java com/americanwell/android/member/activity/setup/AccountNotFoundBecauseNoDTCActivity.java com/americanwell/android/member/activity/setup/ExistingAccountMobileEnrolledActivity.java com/americanwell/android/member/activity/setup/ExistingAccountWebEnrolledActivity.java com/americanwell/android/member/activity/setup/ForgotEmailMemberFoundActivity.java com/americanwell/android/member/activity/setup/ForgotPasswordResetSuccessActivity.java com/americanwell/android/member/activity/setup/MultipleMatchActivity.java com/americanwell/android/member/activity/setup/PartialMatchActivity.java com/americanwell/android/member/fragment/CreateVideoParticipantResponderFragment.java com/americanwell/android/member/fragment/RestClientResponderFragment.java com/americanwell/android/member/fragment/SoapClientResponderFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/americanwell/android/member/fragment/SocialDialogFragment.java com/americanwell/android/member/fragment/StartVidyoEngagementResponderFragment.java com/americanwell/android/member/mvvm/techcheck/view/IntakeTechCheckPermissionsActivity.java com/americanwell/android/member/restws/RestClientService.java com/americanwell/android/member/restws/SoapClientService.java com/americanwell/android/member/util/MessageUtils.java com/americanwell/android/member/util/PDFTools.java com/americanwell/android/member/util/Utils.java com/americanwell/sdk/AWSDKAmWell.java com/americanwell/sdk/internal/d/e/b.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java
00199	Stop recording and release recording resources	record	c/b/a/a/c.java com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java org/webrtc/CameraCapturer.java
00030	Connect to the remote server through the given URL	network	com/americanwell/android/member/util/PDFTools.java
00191	Get messages in the SMS inbox	sms	com/americanwell/android/member/util/PDFTools.java
00036	Get resource file from res/raw directory	reflection	com/americanwell/android/member/activity/SplashActivity.java com/americanwell/android/member/util/MessageUtils.java com/americanwell/android/member/util/PDFTools.java com/americanwell/android/member/util/Utils.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/americanwell/android/member/activity/SplashActivity.java com/americanwell/android/member/activity/appointments/ShowAppointmentDetailActivity.java com/americanwell/android/member/activity/dependent/EditDependentActivity.java com/americanwell/android/member/activity/engagement/AddCreditCardActivity.java com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java com/americanwell/android/member/activity/engagement/YourVisitFragment.java com/americanwell/android/member/activity/messages/AbstractMailboxActivity.java com/americanwell/android/member/activity/messages/AbstractMessageDetailActivity.java com/americanwell/android/member/activity/messages/NewMessageActivity.java com/americanwell/android/member/activity/providers/ShowProviderDetailActivity.java com/americanwell/android/member/restws/RestClientService.java com/americanwell/android/member/restws/SoapClientService.java com/braze/push/BrazeNotificationUtils.java
00022	Open a file from given absolute path of the file	file	bo/app/v5.java c/b/a/a/h.java c/f/a/g0.java com/americanwell/android/member/mvvm/techcheck/viewmodel/IntakeTechCheckViewModel.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java
00013	Read file and put it into a stream	file	bo/app/o0.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java h/p.java i/a/a/g/i.java
00192	Get messages in the SMS inbox	sms	com/americanwell/android/member/util/Utils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/americanwell/android/member/util/Utils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/americanwell/android/member/activity/LoginActivity.java com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java com/americanwell/android/member/activity/settings/ContactActivity.java com/americanwell/android/member/activity/setup/AccessNotEnabledActivity.java com/americanwell/android/member/activity/setup/AccountNotFoundBecauseNoDTCActivity.java com/americanwell/android/member/activity/setup/ExistingAccountMobileEnrolledActivity.java com/americanwell/android/member/activity/setup/ExistingAccountWebEnrolledActivity.java com/americanwell/android/member/activity/setup/ForgotEmailMemberFoundActivity.java com/americanwell/android/member/activity/setup/ForgotPasswordResetSuccessActivity.java com/americanwell/android/member/activity/setup/MultipleMatchActivity.java com/americanwell/android/member/activity/setup/PartialMatchActivity.java com/americanwell/android/member/fragment/RestClientResponderFragment.java com/americanwell/android/member/fragment/SoapClientResponderFragment.java com/americanwell/android/member/util/MessageUtils.java com/americanwell/android/member/util/Utils.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	c/f/a/o.java com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java com/americanwell/android/member/util/Utils.java
00189	Get the content of a SMS message	sms	com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java
00200	Query data from the contact list	collection contact	com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java
00201	Query data from the call log	collection calllog	com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java
00002	Open the camera and take picture	camera	c/b/a/a/c.java
00183	Get current camera parameters and change the setting.	camera	c/b/a/a/c.java org/webrtc/Camera1Session.java
00198	Initialize the recorder and start recording	record	c/b/a/a/c.java com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java
00125	Check if the given file path exist	file	com/americanwell/android/member/util/MessageUtils.java
00056	Modify voice volume	control	com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java com/americanwell/sdk/internal/d/g/a.java org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java
00089	Connect to a URL and receive input stream from the server	command network	c/f/a/f0.java i/a/a/g/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	c/f/a/f0.java i/a/a/g/c.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	c/b/a/a/e.java
00114	Create a secure socket connection to the proxy address	network command	g/i0/f/f.java
00162	Create InetSocketAddress object and connecting to it	socket	com/americanwell/sdk/internal/util/c.java g/i0/j/b.java g/i0/j/h.java
00163	Create new Socket and connecting to it	socket	com/americanwell/sdk/internal/util/c.java g/i0/j/b.java g/i0/j/h.java
00034	Query the current data network type	collection network	com/americanwell/sdk/internal/util/b.java
00064	Monitor incoming call status	control	com/americanwell/sdk/internal/d/g/a.java
00102	Set the phone speaker on	command	com/americanwell/sdk/internal/d/g/a.java
00194	Set the audio source (MIC) and recorded file format	record	com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java
00197	Set the audio encoder and initialize the recorder	record	com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java
00006	Scheduling recording task	record	com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00196	Set the recorded file format and output path	record file	com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java
00078	Get the network operator name	collection telephony	bo/app/m0.java com/americanwell/sdk/internal/d/b/d.java
00195	Set the output path of the recorded file	record file	c/b/a/a/h.java
00007	Use absolute path of directory for the output media file path	file	c/b/a/a/h.java
00033	Query the IMEI number	collection	bo/app/m0.java
00083	Query the IMEI number	collection telephony	bo/app/m0.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/s1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://amwellcloudservices.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/111256039948/namespaces/firebase:fetch?key=AIzaSyC4MMz-ASy_EWU2kPsDQi2SxFTtOWsQc7g. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_PHONE_STATE, android.permission.GET_TASKS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK
Other Common Permissions	5/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY, android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

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
analytics.amwell.systems	ok	**IP:** 18.189.155.62 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
business.amwell.com	ok	**IP:** 172.64.153.179 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
amwellcloudservices.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
blackjack.myonlinecare.com	ok	No Geolocation information available.
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
amwell.com	ok	**IP:** 207.211.47.155 **Country:** United States of America **Region:** Massachusetts **City:** Andover **Latitude:** 42.648373 **Longitude:** -71.161453 **View:** Google Map
accreditnetadmin.urac.org	ok	**IP:** 65.196.93.58 **Country:** United States of America **Region:** Maryland **City:** Gaithersburg **Latitude:** 39.108776 **Longitude:** -77.238350 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
support.tytocare.com	ok	**IP:** 40.112.243.63 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
rest.iad-02.braze.com	ok	**IP:** 172.64.145.177 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
drive.google.com	ok	**IP:** 142.250.9.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
foo@bar.com example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Matomo (Piwik)	Analytics	https://reports.exodus-privacy.eu.org/trackers/138

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"adwords_conversion_key" : "970086441"
"adwords_test_conversion_key" : "963574231"
"awsdk_build_revision" : "abf9adec8738923ce18d0563acfe9ed76732e202"
"awsdk_button_bar_end" : "End"
"awsdk_console_cancel" : "Cancel"
"awsdk_console_cancel_visit_negative" : "No"
"awsdk_console_cancel_visit_positive" : "Yes"
"awsdk_console_end" : "End"
"awsdk_console_extension_negative" : "No"
"awsdk_console_extension_positive" : "Yes"
"awsdk_done_button" : "Done"

POSSIBLE SECRETS
"awsdk_ending_visit_permissions_guest" : "%1$s"
"awsdk_generic_retry" : "Retry"
"awsdk_guest_console_exit" : "Exit"
"awsdk_image_desc_drawer" : "Drawer"
"awsdk_invite_guest_dialog_button_cancel" : "Cancel"
"awsdk_invite_guest_dialog_button_send" : "Send"
"awsdk_invite_guest_list_email_order_eight" : "Eighth"
"awsdk_invite_guest_list_email_order_fifth" : "Fifth"
"awsdk_invite_guest_list_email_order_first" : "First"
"awsdk_invite_guest_list_email_order_fourth" : "Fourth"
"awsdk_invite_guest_list_email_order_ninth" : "Ninth"
"awsdk_invite_guest_list_email_order_second" : "Second"
"awsdk_invite_guest_list_email_order_seventh" : "Seventh"
"awsdk_invite_guest_list_email_order_sixth" : "Sixth"
"awsdk_invite_guest_list_email_order_tenth" : "Tenth"

POSSIBLE SECRETS
"awsdk_invite_guest_list_email_order_third" : "Third"
"awsdk_invite_guest_txt" : "Invite"
"awsdk_lab_result_filename_prefix" : "LabOrderResult"
"awsdk_next_button" : "Next"
"awsdk_reload_txt" : "Reload"
"awsdk_switch_camera_txt" : "Switch"
"awsdk_toggle_bluetooth_txt" : "Bluetooth"
"awsdk_toggle_camera_txt" : "Camera"
"awsdk_toggle_mic_txt" : "Mic"
"awsdk_toggle_speaker_txt" : "Speaker"
"awsdk_tyto_continue_tag" : "Continue"
"awsdk_tyto_live_stream_support_url" : "https://support.tytocare.com"
"awsdk_tyto_password_tag" : "Password"
"awsdk_tyto_show_tag" : "show"
"awsdk_tyto_ssid_tag" : "ssid"

POSSIBLE SECRETS
"awsdk_tyto_txt" : "Tyto"
"awsdk_video_conference_cancel" : "Cancel"
"awsdk_video_conference_leave" : "Leave"
"awsdk_visit_default_guest_display_name" : "Guest"
"awsdk_visit_invite_guest_limit_button_ok" : "OK"
"awsdk_visit_invite_guest_navigation_close_wcag" : "Close"
"awsdk_visit_report_filename_prefix" : "VisitReport"
"awsdktest_remote_service_url" : "https://localhost:1112"
"branch_prod_key" : "key_live_haQhJTWlq2YJzeiVXhE22nhdrrdhKq6n"
"branch_test_key" : "key_test_gkVmKH3lx9ZMudbS9ezX6bejuDcmSq9r"
"com_appboy_api_key" : "222211fc-b6db-45ff-adef-13db3064f8bd"
"com_braze_api_key" : "d745b682-795a-4849-94d5-05f61cf84df3"
"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
"experience_improved_mobile_password" : "Password"
"firebase_database_url" : "https://amwellcloudservices.firebaseio.com"
"google_api_key" : "AIzaSyC4MMz-ASy_EWU2kPsDQi2SxFTtOWsQc7g"
"google_crash_reporting_api_key" : "AIzaSyC4MMz-ASy_EWU2kPsDQi2SxFTtOWsQc7g"
"hasoffers_conversion_key" : "e69b696d277ff57aa5cc9fc61a38842e"
"maps_api_key" : "AIzaSyC029Xth9tJXYolfymgawBNpnhF_ws81uE"
"myAccount_password" : "Password"
"myAccount_username" : "Username"
"online_care_anon_password" : "75State"
"online_care_anon_user" : "OC_MOBILE_DEVICE"
"umbrella_site_restws_password" : "75State"
"umbrella_site_restws_user" : "OC_MOBILE_DEVICE"
sha1/gzF+YoVCU9bXeDGQ7JGQVumRueM=
sha1/7WYxNdMb1OymFMQp4xkGn5TBJlA=
sha1/nKmNAK90Dd2BgNITRaWLjy6UONY=

POSSIBLE SECRETS
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
sha1/GiG0lStik84Ys2XsnA6TTLOB5tQ=
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
sha1/VRmyeKyygdftp6vBg5nDu2kEJLU=
37a6259cc0c1dae299a7866489dff0bd
sha1/PANDaGiVHPNpKri0Jtq6j+ki5b0=
sha1/cTg28gIxU0crbrplRqkQFVggBQk=
sha1/IvGeLsbqzPxdI0b0wuj2xVTdXgc=
sha1/u8I+KQuzKHcdrT6iTb30I70GsD0=
sha1/sYEIGhmkwJQf+uiVKMEkyZs0rMc=
sha1/wHqYaI2J+6sFZAwRfap9ZbjKzE4=
sha1/1S4TwavjSdrotJWU73w4Q2BkZr0=
sha1/aDMOYTWFIVkpg6PI0tLhQG56s8E=
sha1/I0PRSKJViZuUfUYaeX7ATP7RcLc=

PLAYSTORE INFORMATION

Title: Amwell: Doctor Visits 24/7

Score: 3.9594843 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.americanwell.android.member.amwell

Developer Details: American Well, American+Well, None, http://www.americanwell.com, support@americanwell.com,

Release Date: Oct 6, 2013 **Privacy Policy:** Privacy link

Description:

High-quality, affordable medical care is in the palm of your hands — and on-demand — with Amwell. Amwell is the best way to see a doctor from home or on-the-go. Our telehealth app connects you to board-certified, experienced medical providers. High-quality healthcare is now available, 24/7, with on-demand service or scheduled appointments, often with next-day availability. Amwell brings healthcare home through the power of telemedicine so you can feel better faster. AMWELL IS EASY AS 1 -2 - 3 1. Download the app 2. Choose the type of visit 3. Choose your provider No more driving to the doctor or sitting in waiting rooms. With Amwell, quality medical providers are available 24/7, to help you feel better faster. AMWELL DOCTORS HAVE SEEN IT ALL Our experienced clinicians can provide the care you need quickly. Common patients concerns include: • Urgent Care: bronchitis, sinus & respiratory infections, sore throat, diarrhea, cold/flu, gout, strep throat, urinary tract infections, pink eye, hypertension, migraines, pneumonia • Therapy: depression & anxiety, ADHD/ADD, bereavement, trauma, couples therapy, stress, divorce, sleep disorders • Psychiatry: anorexia, bipolar disorder, panic attacks, PTSD, OCD, psychosis, insomnia, substance abuse • Nutrition: weight concerns, food allergies, meal planning, high blood pressure, pediatric nutrition, digestive disorders, pregnancy diets • Lactation Consulting: breastfeeding help AFFORDABLE PRICES FOR SERVICES YOU NEED We believe quality healthcare should be accessible and affordable. That's why before insurance, Amwell costs: • $79 or less for urgent care • $99 starting cost or less for online therapy • $269 initial online psychiatry visit, follow-up visit starting at $99 • $70 or less for nutrition counseling visits • $129 initial breastfeeding support visit, follow-up visit $75 Have health insurance? Many major carriers cover Amwell visits. To check if yours does, simply enter your health insurance information to see the price you will pay for your visit. It's that easy. 100% SECURE & CONFIDENTIAL We take your privacy very seriously. Your visit with the doctor is confidential and HIPAA compliant. AWARDS AND RECOGNITION • Most Popular Mobile Telehealth Platform of 2014-2016 – App Annie • Best Telemedicine App of 2016 – Healthline • First telehealth service awarded accreditation by the American Telemedicine Association CONNECT WITH US To learn more or get your questions answered, please reach out to us! • Web: www.amwell.com • Facebook: www.facebook.com/amwellpatient • Twitter: www.twitter.com/amwell • Email: support@americanwell.com Please note that telehealth is not for emergencies. If you're having a medical emergency, call 911. Any customer review may be used in marketing materials such as emails, fliers, blogs, or other promotional assets. Publishing a review is considered a grant of permission to share the review outside of the App Store. The review will be published anonymously.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:36:13	Generating Hashes	OK

2025-08-29 19:36:13	Extracting APK	OK
2025-08-29 19:36:13	Unzipping	OK
2025-08-29 19:36:14	Parsing APK with androguard	OK
2025-08-29 19:36:14	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:36:14	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:36:16	Parsing AndroidManifest.xml	OK
2025-08-29 19:36:16	Extracting Manifest Data	OK
2025-08-29 19:36:16	Manifest Analysis Started	OK
2025-08-29 19:36:16	Performing Static Analysis on: Amwell (com.americanwell.android.member.amwell)	OK
2025-08-29 19:36:17	Fetching Details from Play Store: com.americanwell.android.member.amwell	OK
2025-08-29 19:36:18	Checking for Malware Permissions	OK

2025-08-29 19:36:18	Fetching icon path	OK
2025-08-29 19:36:18	Library Binary Analysis Started	OK
2025-08-29 19:36:18	Reading Code Signing Certificate	OK
2025-08-29 19:36:19	Running APKiD 2.1.5	OK
2025-08-29 19:36:22	Detecting Trackers	OK
2025-08-29 19:36:24	Decompiling APK to Java with JADX	OK
2025-08-29 19:36:35	Converting DEX to Smali	OK
2025-08-29 19:36:35	Code Analysis Started on - java_source	OK
2025-08-29 19:36:38	Android SBOM Analysis Completed	OK
2025-08-29 19:36:42	Android SAST Completed	OK
2025-08-29 19:36:42	Android API Analysis Started	OK

2025-08-29 19:36:47	Android API Analysis Completed	OK
2025-08-29 19:36:47	Android Permission Mapping Started	OK
2025-08-29 19:36:57	Android Permission Mapping Completed	OK
2025-08-29 19:36:57	Android Behaviour Analysis Started	OK
2025-08-29 19:37:03	Android Behaviour Analysis Completed	OK
2025-08-29 19:37:03	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:37:06	Email and URL Extraction Completed	OK
2025-08-29 19:37:06	Extracting String data from APK	OK
2025-08-29 19:37:06	Extracting String data from Code	OK
2025-08-29 19:37:06	Extracting String values and entropies from Code	OK
2025-08-29 19:37:08	Performing Malware check on extracted domains	OK

2025-08-29 19:37:11	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.