# MOBSF

## ANDROID STATIC ANALYSIS REPORT


MedStar eVisit (13.05.00.000)

| | |
|---|---|
| File Name: | com.medstar.android.promptcare_130500000.apk |
| Package Name: | com.medstar.android.promptcare |
| Scan Date: | Aug. 31, 2025, 3:57 a.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.medstar.android.promptcare_130500000.apk
**Size:** 22.66MB
**MD5:** 822ec18022eac15c621992d090f1e0b9
**SHA1:** 9bc99f47ef69f17b6b40b6388870417ebf3e6e15
**SHA256:** 5c6d88ac03471ac8b2e7aca25320d4d050e067b76552e2a20e1c9265ea98d89d

# APP INFORMATION

**App Name:** MedStar eVisit
**Package Name:** com.medstar.android.promptcare
**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 |
|---|---|---|---|
| com.medstar.android.promptcare.permission.C2D_MESSAGE | unknown | Unknown permission | Unknown permission from android reference |
| 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. |

| 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.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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| 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. |
| 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. |

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

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes.dex | <table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>network operator name check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table> |

| FILE | DETAILS |
| --- | --- |
| classes2.dex | <table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table> |

# BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
| --- | --- |
| com.americanwell.android.member.activity.StartActivity | Schemes: awmedstar://,<br>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<br>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. |
| 2 | Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected.<br>[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.<br>[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/c.java<br>c/a/a/a/e.java<br>c/a/a/a/h.java<br>c/a/a/a/i.java<br>c/b/a/a/c/a.java<br>com/americanwell/android/member/activity/AccessiblityModeActivity.java<br>com/americanwell/android/member/activity/EnterPasscodeActivity.java<br>com/americanwell/android/member/activity/LoginActivity.java<br>com/americanwell/android/member/activity/SplashActivity.java<br>com/americanwell/android/member/activity/TwoFactorAuthenticationActivity.java<br>com/americanwell/android/member/activity/TwoFactorAuthenticationValidationActivity.java<br>com/americanwell/android/member/activity/engagement/CostCheckBeforeEngagementActivity.java<br>com/americanwell/android/member/activity/engagement/MatchmakerActivity.java<br>com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java<br>com/americanwell/android/member/activity/engagement/StartVisitActivity.java<br>com/americanwell/android/member/activity/menudrawer/AbsActionableMenuDrawerItem.java<br>com/americanwell/android/member/activity/menudrawer/AbsMenuDrawerActivity.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<br>OWASP MASVS: MSTG-STORAGE-3 | com/americanwell/android/member/activity/menudrawer/AbsSimpleTextMenuDrawerItem.java<br>com/americanwell/android/member/activity/menudrawer/ActivityMenuDrawerItem.java<br>com/americanwell/android/member/activity/menudrawer/MethodMenuDrawerItem.java<br>com/americanwell/android/member/activity/messages/AbsMessageRelatedActivity.java<br>com/americanwell/android/member/activity/participant/JoinVideoConferenceActivity.java<br>com/americanwell/android/member/activity/participant/WaitingRoomActivity.java<br>com/americanwell/android/member/activity/providers/SpeedPassActivity.java<br>com/americanwell/android/member/activity/settings/MyPreferencesActivity.java<br>com/americanwell/android/member/activity/settings/SettingsActivity.java<br>com/americanwell/android/member/activity/setup/ExperienceImprovedMobileEnrolledActivity.java<br>com/americanwell/android/member/fragment/AWCameraFragment.java<br>com/americanwell/android/member/fragment/FindActiveVisitsResponderFragment.java<br>com/americanwell/android/member/fragment/MatchmakerCreateRequestResponderFragment.java<br>com/americanwell/android/member/fragment/MemberEmailAvailableResponderFragment.java<br>com/americanwell/android/member/util/PDFTools.java<br>com/americanwell/sdk/internal/visitconsole/view/g.java<br>com/braze/support/BrazeLogger.java<br>e/i0/b.java<br>e/i0/h/i/c.java |
| | | | | bo/app/u4.java |

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

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| 2 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | com/americanwell/android/member/fragment/MemberEmailAvailableResponderFragment.java<br>com/americanwell/android/member/fragment/SendMessageInfoResponderFragment.java<br>com/americanwell/android/member/fragment/SendPairingCodeResponderFragment.java<br>com/americanwell/android/member/fragment/ShareExamDataResponderFragment.java<br>com/americanwell/android/member/fragment/UpdateGroupKeyResponderFragment.java<br>com/americanwell/android/member/fragment/UpdateMemberAuthenticationResponderFragment.java<br>com/americanwell/android/member/fragment/UpgradeMemberAuthenticationResponderFragment.java<br>com/americanwell/android/member/fragment/ValidatePairingCodeResponderFragment.java<br>com/americanwell/android/member/fragment/VideoMetricsResponderFragment.java<br>com/americanwell/android/member/fragment/VidyoEngagementResponderFragment.java<br>com/americanwell/android/member/fragment/VidyoEngagementUpdateResponderFragment.java<br>com/americanwell/android/member/location/FetchAddressIntentService.java<br>com/americanwell/android/member/restws/RestClientService.java<br>com/americanwell/android/member/tracking/MatomoTracker.java<br>com/americanwell/android/member/tracking/PropertiesInfoButtonDescription.java<br>com/americanwell/android/member/util/BiometricLoginHelper.java<br>com/americanwell/android/member/util/Constants.java<br>com/americanwell/sdk/entity/SDKErrorReaso |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | n.java<br>com/americanwell/sdk/entity/SDKSuggestion.java<br>com/americanwell/sdk/internal/AWSDKImpl.java<br>com/americanwell/sdk/manager/ValidationConstants.java |
| 3 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | com/braze/configuration/BrazeConfig.java<br>bo/app/e1.java<br>com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java<br>com/americanwell/android/member/activity/participant/WaitingRoomActivity.java<br>com/braze/support/IntentUtils.java<br>g/a/a/e.java |
| 4 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | c/a/a/a/h.java<br>com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java<br>com/americanwell/android/member/util/PDFTools.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 5 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | bo/app/b0.java<br>bo/app/d6.java<br>bo/app/e.java<br>bo/app/f1.java<br>bo/app/g6.java<br>bo/app/h4.java<br>bo/app/l0.java<br>bo/app/l1.java<br>bo/app/m.java<br>bo/app/m0.java<br>bo/app/m6.java<br>bo/app/n0.java<br>bo/app/r3.java<br>bo/app/v5.java<br>bo/app/w4.java<br>bo/app/y0.java<br>com/braze/configuration/RuntimeAppConfigurationProvider.java<br>com/braze/managers/BrazeGeofenceManager.java |
| 6 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | e/i0/h/c.java<br>e/i0/h/d.java<br>e/i0/h/g.java<br>e/i0/h/h.java |
| 7 | 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<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3 | com/americanwell/android/member/activity/chat/AIChatFragment.java<br>com/americanwell/android/member/activity/consumerHome/ConsumerHomeWebViewFragment.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 8 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | com/americanwell/android/member/util/BiometricLoginHelper.java |
| 9 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | com/braze/support/StringUtils.java<br>g/a/a/h/b.java |
| 10 | The file or SharedPreference is World Writable. Any App can write to the file | high | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/americanwell/android/member/util/Utils.java |
| 11 | IP Address disclosure | warning | CWE: CWE-200: Information Exposure<br>OWASP MASVS: MSTG-CODE-2 | com/medstar/android/promptcare/BuildConfig.java |

# NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|

# BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/americanwell/android/member/activity/BaseManagePermissionsActivity.java<br>com/americanwell/android/member/activity/LoginActivity.java<br>com/americanwell/android/member/activity/SplashActivity.java<br>com/americanwell/android/member/activity/WebViewActivity.java<br>com/americanwell/android/member/activity/consumerHome/ConsumerHomeActivity.java<br>com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java<br>com/americanwell/android/member/activity/engagement/StartVisitActivity.java<br>com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java<br>com/americanwell/android/member/activity/engagement/tytoLiveStream/TytoLiveStreamQRStatusFragment.java<br>com/americanwell/android/member/activity/settings/AboutActivity.java<br>com/americanwell/android/member/activity/settings/ContactActivity.java<br>com/americanwell/android/member/activity/setup/AccessNotEnabledActivity.java<br>com/americanwell/android/member/activity/setup/AccountNotFoundBecauseNoDTCActivity.java<br>com/americanwell/android/member/activity/setup/ExistingAccountMobileEnrolledActivity.java<br>com/americanwell/android/member/activity/setup/ExistingAccountWebEnrolledActivity.java<br>com/americanwell/android/member/activity/setup/ForgotEmailMemberFoundActivity.java<br>com/americanwell/android/member/activity/setup/ForgotPasswordResetSuccessActivity.java<br>com/americanwell/android/member/activity/setup/MultipleMatchActivity.java<br>com/americanwell/android/member/activity/setup/PartialMatchActivity.java<br>com/americanwell/android/member/fragment/CreateVideoParticipantResponderFragment.java<br>com/americanwell/android/member/fragment/RestClientResponderFragment.java<br>com/americanwell/android/member/fragment/SoapClientResponderFragment.java<br>com/americanwell/android/member/fragment/SocialDialogFragment.java<br>com/americanwell/android/member/fragment/StartVidyoEngagementResponderFragment.java<br>com/americanwell/android/member/mvvm/techcheck/view/IntakeTechCheckPermissionsActivity.java<br>com/americanwell/android/member/restws/RestClientService.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| | | | com/americanwell/android/member/restws/SoapClientService.java<br>com/americanwell/android/member/util/MessageUtils.java<br>com/americanwell/android/member/util/PDFTools.java<br>com/americanwell/android/member/util/Utils.java |
| | | | com/americanwell/sdk/AWSDKAmWell.java<br>com/americanwell/sdk/internal/d/e/b.java<br>com/braze/Braze.java<br>com/braze/push/BrazeNotificationUtils.java<br>com/braze/ui/support/UriUtils.java |
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | com/americanwell/android/member/activity/LoginActivity.java<br>com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java<br>com/americanwell/android/member/activity/settings/ContactActivity.java<br>com/americanwell/android/member/activity/setup/AccessNotEnabledActivity.java<br>com/americanwell/android/member/activity/setup/AccountNotFoundBecauseNoDTCActivity.java<br>com/americanwell/android/member/activity/setup/ExistingAccountMobileEnrolledActivity.java<br>com/americanwell/android/member/activity/setup/ExistingAccountWebEnrolledActivity.java<br>com/americanwell/android/member/activity/setup/ForgotEmailMemberFoundActivity.java<br>com/americanwell/android/member/activity/setup/ForgotPasswordResetSuccessActivity.java<br>com/americanwell/android/member/activity/setup/MultipleMatchActivity.java<br>com/americanwell/android/member/activity/setup/PartialMatchActivity.java<br>com/americanwell/android/member/fragment/RestClientResponderFragment.java<br>com/americanwell/android/member/fragment/SoapClientResponderFragment.java<br>com/americanwell/android/member/util/MessageUtils.java<br>com/americanwell/android/member/util/Utils.java |
| 00056 | Modify voice volume | control | com/americanwell/android/member/activity/engagement/WaitingRoomActivity.java<br>com/americanwell/sdk/internal/d/g/a.java<br>org/webrtc/audio/WebRtcAudioTrack.java<br>org/webrtc/voiceengine/WebRtcAudioTrack.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 |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/americanwell/android/member/activity/engagement/AttachDocumentHelper.java<br>com/americanwell/android/member/util/Utils.java |
| 00013 | Read file and put it into a stream | file | bo/app/o0.java<br>com/braze/support/BrazeImageUtils.java<br>com/braze/support/WebContentUtils.java<br>f/p.java<br>g/a/a/g/i.java |
| 00162 | Create InetSocketAddress object and connecting to it | socket | com/americanwell/sdk/internal/util/c.java<br>e/i0/h/b.java<br>e/i0/h/h.java |
| 00163 | Create new Socket and connecting to it | socket | com/americanwell/sdk/internal/util/c.java<br>e/i0/h/b.java<br>e/i0/h/h.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00091 | Retrieve data from broadcast | collection | com/americanwell/android/member/activity/SplashActivity.java<br>com/americanwell/android/member/activity/appointments/ShowAppointmentDetailActivity.java<br>com/americanwell/android/member/activity/dependent/EditDependentActivity.java<br>com/americanwell/android/member/activity/engagement/AddCreditCardActivity.java<br>com/americanwell/android/member/activity/engagement/PaymentInfoActivity.java<br>com/americanwell/android/member/activity/engagement/YourVisitFragment.java<br>com/americanwell/android/member/activity/messages/AbstractMailboxActivity.java<br>com/americanwell/android/member/activity/messages/AbstractMessageDetailActivity.java<br>com/americanwell/android/member/activity/messages/NewMessageActivity.java<br>com/americanwell/android/member/activity/providers/ShowProviderDetailActivity.java<br>com/americanwell/android/member/restws/RestClientService.java<br>com/americanwell/android/member/restws/SoapClientService.java<br>com/braze/push/BrazeNotificationUtils.java |
| 00036 | Get resource file from res/raw directory | reflection | com/americanwell/android/member/activity/SplashActivity.java<br>com/americanwell/android/member/util/MessageUtils.java<br>com/americanwell/android/member/util/PDFTools.java<br>com/americanwell/android/member/util/Utils.java<br>com/braze/push/BrazeNotificationUtils.java<br>com/braze/ui/support/UriUtils.java |
| 00022 | Open a file from given absolute path of the file | file | bo/app/v5.java<br>c/a/a/a/h.java<br>com/americanwell/android/member/mvvm/techcheck/viewmodel/IntakeTechCheckViewModel.java<br>com/braze/support/BrazeImageUtils.java<br>com/braze/support/WebContentUtils.java |
| 00125 | Check if the given file path exist | file | com/americanwell/android/member/util/MessageUtils.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00183 | Get current camera parameters and change the setting. | camera | c/a/a/a/c.java<br>org/webrtc/Camera1Session.java |
| 00208 | Capture the contents of the device screen | collection screen | org/webrtc/ScreenCapturerAndroid.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 |
| 00199 | Stop recording and release recording resources | record | c/a/a/a/c.java<br>com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.java<br>org/webrtc/CameraCapturer.java |
| 00198 | Initialize the recorder and start recording | record | c/a/a/a/c.java<br>com/americanwell/android/member/mvvm/techcheck/manager/TechCheckMicManager.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 |
| 00123 | Save the response to JSON after connecting to the remote server | network command | bo/app/s1.java |
| 00195 | Set the output path of the recorded file | record file | c/a/a/a/h.java |
| 00007 | Use absolute path of directory for the output media file path | file | c/a/a/a/h.java |
| 00002 | Open the camera and take picture | camera | c/a/a/a/c.java |
| 00001 | Initialize bitmap object and compress data (e.g. JPEG) into bitmap object | camera | c/a/a/a/e.java |
| 00078 | Get the network operator name | collection telephony | bo/app/m0.java<br>com/americanwell/sdk/internal/d/b/d.java |
| 00033 | Query the IMEI number | collection | bo/app/m0.java |
| 00083 | Query the IMEI number | collection telephony | bo/app/m0.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 |

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00112 | Get the date of the calendar event | collection calendar | com/americanwell/android/member/activity/dependent/EditDependentActivity.java<br>com/americanwell/android/member/activity/healthplan/HealthPlanFragment.java<br>com/americanwell/android/member/util/Utils.java<br>com/americanwell/sdk/entity/SDKLocalDate.java |
| 00192 | Get messages in the SMS inbox | sms | com/americanwell/android/member/util/Utils.java |
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | com/americanwell/android/member/util/Utils.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | g/a/a/g/c.java |
| 00109 | Connect to a URL and get the response code | network command | g/a/a/g/c.java |

# FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
| --- | --- | --- |
| App talks to a Firebase database | info | The app talks to Firebase database at https://evisit-12e82.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/793661373849/namespaces/firebase:fetch?key=AIzaSyCGa8R0_12DJVS8bbiFpiqD017ppu1VGL0. 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<br>**Country:** United States of America<br>**Region:** Ohio<br>**City:** Columbus<br>**Latitude:** 39.961182<br>**Longitude:** -82.998787<br>**View:** Google Map |
| business.amwell.com | ok | **IP:** 104.18.34.77<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |
| www.americanwell.com | ok | **IP:** 13.224.53.29<br>**Country:** United States of America<br>**Region:** Arizona<br>**City:** Phoenix<br>**Latitude:** 33.448380<br>**Longitude:** -112.074043<br>**View:** Google Map |
| twitter.com | ok | **IP:** 172.66.0.227<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| blackjack.myonlinecare.com | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| www.medstarhealth.org | ok | **IP:** 13.107.246.71<br>**Country:** Netherlands<br>**Region:** Noord-Holland<br>**City:** Amsterdam<br>**Latitude:** 52.374031<br>**Longitude:** 4.889690<br>**View:** Google Map |
| www.braze.com | ok | **IP:** 104.17.227.60<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| amwell.com | ok | **IP:** 207.211.47.155<br>**Country:** United States of America<br>**Region:** Massachusetts<br>**City:** Andover<br>**Latitude:** 42.648373<br>**Longitude:** -71.161453<br>**View:** Google Map |
| accreditnetadmin.urac.org | ok | **IP:** 65.196.93.58<br>**Country:** United States of America<br>**Region:** Maryland<br>**City:** Gaithersburg<br>**Latitude:** 39.108776<br>**Longitude:** -77.238350<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| sdk.iad-01.braze.com | ok | **IP:** 172.64.148.188<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |
| medstar-evisit.com | ok | **IP:** 104.21.16.1<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| support.tytocare.com | ok | **IP:** 40.112.243.63<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.774929<br>**Longitude:** -122.419418<br>**View:** Google Map |
| drive.google.com | ok | **IP:** 216.58.215.46<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| sondheim.braze.com | ok | **IP:** 104.18.43.4<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |
| evisit-12e82.firebaseio.com | ok | **IP:** 34.120.206.254<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| github.com | ok | **IP:** 140.82.112.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

## EMAILS

| EMAIL | FILE |
| --- | --- |
| telehealthsupport@medstar.net<br>foo@bar.com<br>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_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" |

| POSSIBLE SECRETS |
| --- |
| "awsdk_console_end" : "End" |
| "awsdk_console_extension_negative" : "No" |
| "awsdk_console_extension_positive" : "Yes" |
| "awsdk_done_button" : "Done" |
| "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" |

| POSSIBLE SECRETS |
| --- |
| "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" |
| "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" |

| POSSIBLE SECRETS |
| --- |
| "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" |
| "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" : "6a9f664a-da5e-4fe4-af0e-6324e66b0c0e" |

| POSSIBLE SECRETS |
| --- |
| "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" |
| "experience_improved_mobile_password" : "Password" |
| "firebase_database_url" : "https://evisit-12e82.firebaseio.com" |
| "google_api_key" : "AIzaSyCGa8R0_12DJVS8bbiFpiqD017ppu1VGL0" |
| "google_crash_reporting_api_key" : "AIzaSyCGa8R0_12DJVS8bbiFpiqD017ppu1VGL0" |
| "hasoffers_conversion_key" : "5a050ac597a020d1e345c5c8f8b9a1f0" |
| "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" |

| POSSIBLE SECRETS |
| --- |
| sha1/gzF+YoVCU9bXeDGQ7JGQVumRueM= |
| sha1/7WYxNdMb1OymFMQp4xkGn5TBJlA= |
| sha1/nKmNAK90Dd2BgNITRaWLjy6UONY= |
| c06c8400-8e06-11e0-9cb6-0002a5d5c51b |
| sha1/GiG0lStik84Ys2XsnA6TTLOB5tQ= |
| bb392ec0-8d4d-11e0-a896-0002a5d5c51b |
| sha1/VRmyeKyygdftp6vBg5nDu2kEJLU= |
| 37a6259cc0c1dae299a7866489dff0bd |
| sha1/PANDaGiVHPNpKri0Jtq6j+ki5b0= |
| sha1/cTg28gIxU0crbrplRqkQFVggBQk= |
| sha1/IvGeLsbqzPxdI0b0wuj2xVTdXgc= |
| sha1/u8l+KQuzKHcdrT6iTb30I70GsD0= |
| sha1/sYEIGhmkwJQf+uiVKMEkyZs0rMc= |
| sha1/wHqYaI2J+6sFZAwRfap9ZbjKzE4= |
| sha1/1S4TwavjSdrotJWU73w4Q2BkZr0= |

| POSSIBLE SECRETS |
| --- |
| sha1/aDMOYTWFIVkpg6PI0tLhQG56s8E= |
| sha1/I0PRSKJViZuUfUYaeX7ATP7RcLc= |

# PLAYSTORE INFORMATION

**Title:** MedStar eVisit – Telehealth

**Score:** 4.22 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.medstar.android.promptcare

**Developer Details:** MedStar Health, 8479049399463248492, None, http://medstarhealth.org, web@medstar.net,

**Release Date:** Jul 31, 2015 **Privacy Policy:** Privacy link

**Description:**

MedStar eVisit-Telehealth: 24/7 Urgent Care Need secure, fast, reliable urgent care? MedStar eVisit - Telehealth connects you with a trusted urgent care provider anytime—no appointment needed! Skip the waiting room and start a secure virtual visit with a trusted health care provider from your phone, tablet, or computer. Care When and Where You Need It: · Available 24/7, 365 days a year. · Most insurance plans accepted, just pay your regular co-pay. · Self pay is just $79. · Easy sign-up within minutes. Our experienced providers can provide the care you need quickly. Common conditions treated include: · Cold/flu, COVID-19, sinus infections, Gout, Sore throat, pink eye, seasonal allergies, rash or hives, tick bites, nausea, vomiting, and/or diarrhea, headache, migraines, urinary tract infections (females 18+), back or joint pain, insect, animal or human bites, minor falls, minor motor vehicle accidents Must be physically located in Maryland, Virginia, or Washington D.C. at the time of care. Convenient, affordable urgent care is at your fingertips with three easy steps: 1. Download the eVisit - telehealth app 2. Sign up 3. See a provider Download now and be ready to get the care you need, when you need it - an online MedStar Health provider is only a click away! To learn more or get your questions answered, please reach out to us! Web: https://www.medstarhealth.org/services/medstar-evisit-telehealth Email: medstar-evisit@medstar.net For your convenience, MedStar eVisit uses the MedStar Health Patient Portal to record the results of your visit. You will see it along with all of your other MedStar Health visit information from our other providers and specialists. If you use Apple Health, you can choose to share your health information, such as heart rate, blood pressure, body temperature, blood glucose levels, weight, nutritional information, and respiratory rate, with the provider during your virtual video visit. MedStar eVisit – Telehealth takes your privacy seriously. Your visit with the provider is secure and HIPAA compliant. MedStar Health's physicians, nurse practitioners, physician assistants, nurses, researchers, and support staff are all focused on one thing — caring for you and your family. Our 30,000 associates and 6,000 affiliated physicians support MedStar Health's patient-first philosophy of care, compassion, clinical excellence, and customer service. We proudly care for more than half a million patients each year across Maryland and the Washington, D.C., region in our hospitals, urgent care centers, ambulatory centers, and physician offices. Our extensive network of providers enables us to offer the highest quality, most advanced care – close to where our patients live and work. And, because we are committed to our not-for-profit mission, we remain dedicated to reinvesting in the health and wellness of all the communities we serve.

# SCAN LOGS

| Timestamp | Event | Error |
|---|---|---|
| 2025-08-31 03:57:51 | Generating Hashes | OK |
| 2025-08-31 03:57:51 | Extracting APK | OK |
| 2025-08-31 03:57:51 | Unzipping | OK |
| 2025-08-31 03:57:51 | Parsing APK with androguard | OK |
| 2025-08-31 03:57:51 | Extracting APK features using aapt/aapt2 | OK |
| 2025-08-31 03:57:51 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-08-31 03:57:54 | Parsing AndroidManifest.xml | OK |
| 2025-08-31 03:57:54 | Extracting Manifest Data | OK |
| 2025-08-31 03:57:54 | Manifest Analysis Started | OK |

| | | |
|---|---|---|
| 2025-08-31 03:57:54 | Performing Static Analysis on: MedStar eVisit (com.medstar.android.promptcare) | OK |
| 2025-08-31 03:57:55 | Fetching Details from Play Store: com.medstar.android.promptcare | OK |
| 2025-08-31 03:57:57 | Checking for Malware Permissions | OK |
| 2025-08-31 03:57:57 | Fetching icon path | OK |
| 2025-08-31 03:57:57 | Library Binary Analysis Started | OK |
| 2025-08-31 03:57:57 | Reading Code Signing Certificate | OK |
| 2025-08-31 03:57:57 | Running APKiD 2.1.5 | OK |
| 2025-08-31 03:58:01 | Detecting Trackers | OK |
| 2025-08-31 03:58:03 | Decompiling APK to Java with JADX | OK |
| 2025-08-31 03:58:17 | Converting DEX to Smali | OK |
| 2025-08-31 03:58:17 | Code Analysis Started on - java_source | OK |

| | | |
|---|---|---|
| 2025-08-31 03:58:23 | Android SBOM Analysis Completed | OK |
| 2025-08-31 03:58:29 | Android SAST Completed | OK |
| 2025-08-31 03:58:29 | Android API Analysis Started | OK |
| 2025-08-31 03:58:36 | Android API Analysis Completed | OK |
| 2025-08-31 03:58:36 | Android Permission Mapping Started | OK |
| 2025-08-31 03:58:47 | Android Permission Mapping Completed | OK |
| 2025-08-31 03:58:47 | Android Behaviour Analysis Started | OK |
| 2025-08-31 03:58:55 | Android Behaviour Analysis Completed | OK |
| 2025-08-31 03:58:55 | Extracting Emails and URLs from Source Code | OK |
| 2025-08-31 03:58:57 | Email and URL Extraction Completed | OK |
| 2025-08-31 03:58:57 | Extracting String data from APK | OK |

| | | |
|---|---|---|
| 2025-08-31 03:58:57 | Extracting String data from Code | OK |
| 2025-08-31 03:58:57 | Extracting String values and entropies from Code | OK |
| 2025-08-31 03:59:00 | Performing Malware check on extracted domains | OK |
| 2025-08-31 03:59:05 | 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.