MOBSF

ANDROID STATIC ANALYSIS REPORT

MyMethodist (2.5.2)

File Name:	org.houstonmethodist.methodistmobile_218.apk
Package Name:	org.houstonmethodist.methodistmobile
Scan Date:	Sept. 1, 2025, 3:07 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	29	4	2	2

FILE INFORMATION

File Name: org.houstonmethodist.methodistmobile_218.apk
Size: 63.76MB
MD5: 425155f33a4a656390e0216872db7b2e
SHA1: b70a255ff267ab89bfa1ddfac6c89e1eef2fa5f4
SHA256: d6dbf36e582213c10229eba1ab3976ece14cdf49fd52d5fa2a08a2047d1e1750

APP INFORMATION

App Name: MyMethodist
Package Name: org.houstonmethodist.methodistmobile
Main Activity: org.houstonmethodist.methodistmobile.home.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 2.5.2

Android Version Code: 218

APP COMPONENTS

Activities: 140

Services: 18

Receivers: 7

Providers: 3

Exported Activities: 12

Exported Services: 2

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-02-01 20:25:47+00:00
Valid To: 2048-02-01 20:25:47+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x20347a78e2f74cf42b0ef935bbd2df6d1809eaa0
Hash Algorithm: sha256
md5: 2650bdf64b91041ba7265a1efd4bfdeb
sha1: 8495bce4e14e842f11c54e827c12b02b685a4347
sha256: dd3e5f292ffbfe0058553344232eacc1e106ca88746ab30ebf620e479869e27b
sha512: fc11587e9bd4167a679d4f90e36e0fc3b3a81c71cfe254398d9da766a77d0e014f00ae44f525cba649302dd150261af1208def3d3091408c8b44043e3ef4775e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 91b78f83f1a36d64bc882d55eb2c9a4056a0145d5e4a9a1c38e8168197a171d5
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
org.houstonmethodist.methodistmobile.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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>425155f33a4a656390e0216872db7b2e.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
epic.mychart.android.library.prelogin.SplashActivity	Schemes: hmmychart://,

ACTIVITY	INTENT
org.houstonmethodist.methodistmobile.home.MainActivity	Schemes: https://, hmapp://, mymethodist://, hmadobe://, Hosts: th.uat.houstonmethodistcare.org, th.houstonmethodistcare.org, mymethodist.page.link, houstonmethodist.page.link, scheduling.houstonmethodistcare.org, scheduling.uat.houstonmethodistcare.org, virtual, *, Path Prefixes: /visit, /virtual,
org.houstonmethodist.dexcare.activity.DexCareAuth0Activity	Schemes: dexcare://, Hosts: auth,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /org.houstonmethodist.methodistmobile,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /org.houstonmethodist.methodistmobile,
com.auth0.android.provider.RedirectActivity	Schemes: hmauth://, Hosts: @string/auth0_domain, Path Prefixes: /android/org.houstonmethodist.methodistmobile/callback,

NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **1**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.

NO	SCOPE	SEVERITY	DESCRIPTION
2	test.methodistmobileapi.houstonmethodist.org testphysician.houstonmethodist.org uat.secondopinion.houstonmethodist.org	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **17** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (org.houstonmethodist.methodistmobile.home.LandingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (epic.mychart.android.library.prelogin.SplashActivity) 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.
5	Activity (org.houstonmethodist.methodistmobile.home.MainActivity) 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 (epic.mychart.android.library.healthlinks.HealthConnectPrivacyPolicyActivity) 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-Alias (epic.mychart.android.library.HealthConnectViewPermissionsActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.
8	Activity (org.houstonmethodist.dexcare.activity.DexCareAuth0Activity) 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
9	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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.
10	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity (com.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.
12	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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.
15	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Activity (androidx.test.core.app.InstrumentationActivityInvoker$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.
17	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
18	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: **9** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				android/content/compose/a.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONDefinition.java com/auth0/android/callback/Auth0ViewModel.java com/auth0/android/callback/DashboardViewModel.java com/auth0/android/callback/ServiceOfflineViewModel.java com/bumptech/glide/load/d.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/v.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/EnterPasscodeDialogFragment.java com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/LoginHelper.java com/epic/patientengagement/authentication/login/utilities/LoginResultCode.java com/epic/patientengagement/authentication/login/utilities/OrganizationLoginHelper.java com/epic/patientengagement/authentication/login/utilities/SamlSessionManager.java com/epic/patientengagement/core/component/IAuthenticationComponentAPI.java com/epic/patientengagement/core/deeplink/DeepLinkLaunchParameters.java com/epic/patientengagement/core/mychartweb/ExternalJumpDialogFragment.java com/epic/patientengagement/core/mychartweb/MyChartWebQueryParameters.java com/epic/patientengagement/core/mychartweb/MyChartWebViewClient.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/mychartweb/WebSessionWebServiceAPI.java com/epic/patientengagement/core/onboarding/OnboardingHostFragment.java com/epic/patientengagement/core/onboarding/OnboardingPageFragment.java com/epic/patientengagement/core/permission

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames,	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering	s/PermissionProminentDisclosure.java com/epic/patientengagement/core/ui/VideoCardView.java com/epic/patientengagement/core/utilities/PrintUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/epic/patientengagement/core/utilities/file/FileChooserTypeSelectionDialogFragment.java com/epic/patientengagement/core/webservice/WebService.java com/epic/patientengagement/core/webservice/processor/MyChartResponseProcessor.java com/epic/patientengagement/homepage/HomePageComponentAPI.java com/launchdarkly/sdk/LDContext.java com/opentok/android/DefaultAudioDevice.java com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java com/stripe/android/auth/PaymentBrowserAuthContract.java com/stripe/android/core/networking/ApiRequest.java com/stripe/android/googlepaylauncher/Args.java com/stripe/android/googlepaylauncher/PaymentIntentArgs.java com/stripe/android/googlepaylauncher/SetupIntentArgs.java com/stripe/android/link/serialization/PopupPayload.java com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/CreateFinancialCon

NO	ISSUE	SEVERITY	STANDARDS	FILES
	passwords, keys etc.		OWASP MASVS: MSTG-STORAGE-14	nectionsSessionParams.java com/stripe/android/model/ElementsSessionParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/RadarSessionWithHCaptcha.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Source.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/model/StripeIntent.java com/stripe/android/payments/Unvalidated.java com/stripe/android/payments/Validated.java com/stripe/android/payments/bankaccount/navigation/CollectBankAccountContract.java com/stripe/android/payments/bankaccount/ui/a.java com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract.java com/stripe/android/paymentsheet/CustomerConfiguration.java com/stripe/android/paymentsheet/PaymentSheet$InitializationMode.java com/stripe/android/paymentsheet/flowcontroller/Args.java com/stripe/android/polling/c.java com/stripe/android/stripe3ds2/observability/b.java com/stripe/android/stripe3ds2/transaction/AcsData.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/transaction/IntentData.java epic/mychart/android/library/api/classes/WPAPIAuthentication.java epic/mychart/android/library/healthlinks/d.java org/altbeacon/beacon/service/MonitoringData.java org/altbeacon/beacon/service/RangingData.java org/altbeacon/beacon/service/SettingsData.java org/altbeacon/beacon/service/StartRMData.java org/dexcare/DexCareSDK.java org/dexcare/services/internalservices/schedule/models/TokboxVisit.java org/dexcare/services/patient/models/MyChartLinkCreds.java org/dexcare/services/practices/models/PracticePaymentAvailability.java org/dexcare/services/provider/models/ScheduledProviderVisit.java org/dexcare/services/virtualvisit/models/AdditionalDetailsV9.java org/dexcare/services/virtualvisit/models/WaitTimeLocalizationInfo.java org/dexcare/services/virtualvisit/video/models/SessionInfo.java org/houstonmethodist/methodistmobile/contacts/activity/a.java org/houstonmethodist/methodistmobile/home/c0.java org/houstonmethodist/scheduling/api/ProviderApiLogIn.java org/houstonmethodist/scheduling/fad/service/IFADRecentHistoryServiceKt.java org/houstonmethodist/scheduling/model/service/IFADRecentHistoryServiceKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ice/IPADRecentHistoryServiceKt.java org/koin/dsl/internalservices/schedule/models/TokboxVisit.java org/koin/dsl/patient/models/MyChartLinkCreds.java org/koin/dsl/practices/models/PracticePaymentAvailability.java org/koin/dsl/provider/models/ScheduledProviderVisit.java org/koin/dsl/virtualvisit/models/AdditionalDetailsV9.java org/koin/dsl/virtualvisit/models/WaitTimeLocalizationInfo.java org/koin/dsl/virtualvisit/video/models/SessionInfo.java
2	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	com/bumptech/glide/b.java com/bumptech/glide/disklrucache/a.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/gifdecoder/e.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/mediastore/e.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/bitmap_recycle/i.java com/bumptech/glide/load/engine/bitmap_recycle/j.java com/bumptech/glide/load/engine/cache/e.java com/bumptech/glide/load/engine/cache/i.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/engine/x.java com/bumptech/glide/load/model/s.java com/bumptech/glide/load/resource/a.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/k.java com/bumptech/glide/load/resource/bitmap/l.java com/bumptech/glide/load/resource/bitmap/p.java com/bumptech/glide/load/resource/bitmap/x.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/l.java com/bumptech/glide/module/d.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/i.java com/bumptech/glide/util/pool/a.java com/epic/patientengagement/core/utilities/PerformanceLogger.java com/jakewharton/disklrucache/a.java com/opentok/android/BaseVideoCapturer.java epic/mychart/android/library/utilities/r.java org/koin/core/logger/a.java timber/log/a.java
3	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/adobe/marketing/mobile/assurance/AssuranceWebViewSocket.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/pierfrancescosoffritti/androidyoutubeplayer/core/player/views/WebViewYouTubePlayer.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/epic/patientengagement/pdfviewer/pdf/PdfFile.java epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/k.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/launchdarkly/eventsource/n.java org/dexcare/dal/network/RetrofitFactory.java org/houstonmethodist/methodistmobile/common/l.java org/koin/dsl/ServiceManager.java
7	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	com/adobe/marketing/mobile/internal/eventhub/history/b.java com/adobe/marketing/mobile/internal/util/SQLiteDatabaseHelper.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/auth0/android/authentication/storage/f.java
9	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	com/epic/patientengagement/core/utilities/EncryptionUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java epic/mychart/android/library/utilities/DeviceUtil.java
11	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/epic/patientengagement/homepage/itemfeed/webservice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/QuestionnaireSeries.java epic/mychart/android/library/utilities/r.java
12	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/airbnb/lottie/network/f.java epic/mychart/android/library/utilities/k.java
13	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.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	android/content/a.java android/content/o.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/assurance/AssuranceExtension.java com/adobe/marketing/mobile/services/ui/a.java com/auth0/android/provider/BrowserPicker.java com/auth0/android/provider/n.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/PreloginDeeplinkManager.java com/epic/patientengagement/core/extensibility/ExtensibilityLaunchManager.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/utilities/IntentUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/kizitonwose/calendar/view/NavigationHelperKt.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/k.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/campaigns/c.java epic/mychart/android/library/community/WebCommunityManageMyAccountsActivity.java epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/general/DeepLinkManager.java epic/mychart/android/library/general/FDILauncherActivity.java epic/mychart/android/library/general/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
			epic/mychart/android/library/healthlinks/l.java epic/mychart/android/library/insurance/e.java epic/mychart/android/library/letters/WebLettersActivity.java epic/mychart/android/library/personalize/c.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/todo/PatientAssignedQuestionnaireWebViewActivity.java epic/mychart/android/library/utilities/CommunityUtil.java epic/mychart/android/library/utilities/k.java epic/mychart/android/library/welcomewizard/WelcomeWizardWebViewFragmentManager.java org/houstonmethodist/methodistmobile/common/g.java org/houstonmethodist/methodistmobile/utils/a.java org/houstonmethodist/scheduling/mammo/MammoAdapter.java org/houstonmethodist/scheduling/model/SameDayClinicAdapter.java org/houstonmethodist/scheduling/model/SameDayClinicDetailPopUpFactory.java org/houstonmethodist/scheduling/model/additional/FadAdditionalSlotsFragment$observe$17.java org/houstonmethodist/scheduling/model/profile/OfficeLocationAdapter.java org/houstonmethodist/scheduling/model/service/ProviderListAdapter.java org/houstonmethodist/scheduling/util/NavigationHelperKt.java org/koin/dsl/virtualvisit/video/AlertManager.java
00056	Modify voice volume	control	com/vonage/webrtc/voiceengine/WebRtcAudioTrack.java
00036	Get resource file from res/raw directory	reflection	android/content/a.java com/auth0/android/provider/n.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/prelogin/WebServer.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/utilities/k.java org/houstonmethodist/methodistmobile/common/g.java org/koin/dsl/virtualvisit/video/AlertManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	android/content/core/l.java com/adobe/marketing/mobile/internal/util/c.java com/airbnb/lottie/network/f.java com/airbnb/lottie/network/g.java com/airbnb/lottie/r.java com/epic/patientengagement/core/utilities/DeviceUtil.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java com/launchdarkly/sdk/android/q0.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java org/altbeacon/beacon/service/ScanState.java
00013	Read file and put it into a stream	file	android/content/core/l.java com/adobe/marketing/mobile/internal/util/c.java com/adobe/marketing/mobile/launch/rulesengine/download/c.java com/adobe/marketing/mobile/services/internal/caching/b.java com/airbnb/lottie/network/f.java com/airbnb/lottie/network/g.java com/bumptech/glide/disklrucache/a.java com/bumptech/glide/load/b.java com/bumptech/glide/load/model/f.java com/epic/patientengagement/pdfviewer/utilities/FileUtils.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/jakewharton/disklrucache/a.java epic/mychart/android/library/customobjects/StoredFile.java epic/mychart/android/library/customviews/PhotoViewerActivity.java epic/mychart/android/library/utilities/DeviceUtil.java epic/mychart/android/library/utilities/i.java okio/q.java org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java org/altbeacon/beacon/service/MonitoringStatus.java org/altbeacon/beacon/service/ScanState.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	android/content/a.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/a.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/k.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java org/houstonmethodist/methodistmobile/common/g.java
00091	Retrieve data from broadcast	collection	com/adobe/marketing/mobile/LocalNotificationHandler.java com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/stripe/android/link/LinkForegroundActivity.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/billing/PaymentConfirmationActivity.java epic/mychart/android/library/billing/RecentStatementActivity.java epic/mychart/android/library/healthadvisories/HealthAdvisoryMarkCompleteActivity.java epic/mychart/android/library/medications/MedRefillActivity.java epic/mychart/android/library/messages/ComposeActivity.java epic/mychart/android/library/personalize/PersonalizeFragment.java epic/mychart/android/library/springboard/CustomWebModeJumpActivity.java epic/mychart/android/library/testresults/TestResultDetailActivity.java
00096	Connect to a URL and set request method	command network	com/adobe/marketing/mobile/assurance/a.java com/airbnb/lottie/network/b.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/stripe/android/core/networking/f.java com/stripe/android/stripe3ds2/transaction/y.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/marketing/mobile/assurance/a.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/stripe/android/stripe3ds2/transaction/y.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00109	Connect to a URL and get the response code	network command	com/adobe/marketing/mobile/assurance/a.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/stripe/android/stripe3ds2/transaction/y.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00153	Send binary data over HTTP	http	com/adobe/marketing/mobile/assurance/a.java epic/mychart/android/library/utilities/g.java
00130	Get the current WIFI information	wifi collection	org/dexcare/dal/exts/ContextExtsKt.java org/koin/dsl/virtualvisit/video/TytoCareUi.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/k.java
00094	Connect to a URL and read data from it	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/healthlinks/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/b.java com/bumptech/glide/load/data/j.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/stripe/android/stripe3ds2/transaction/y.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00175	Get notification manager and cancel notifications	notification	org/koin/dsl/virtualvisit/video/fragment/VirtualVisitFragment.java
00108	Read the input stream from given URL	network command	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customobjects/a.java
00102	Set the phone speaker on	command	com/opentok/android/DefaultAudioDevice.java
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java
00028	Read file from assets directory	file	com/opentok/android/PublisherKit.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/assurance/b.java com/adobe/marketing/mobile/services/h.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/r.java epic/mychart/android/library/messages/Attachment.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00202	Make a phone call	control	epic/mychart/android/library/utilities/k.java org/houstonmethodist/methodistmobile/common/g.java
00203	Put a phone number into an intent	control	epic/mychart/android/library/utilities/k.java org/houstonmethodist/methodistmobile/common/g.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/c.java
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java
00208	Capture the contents of the device screen	collection screen	com/vonage/webrtc/ScreenCapturerAndroid.java
00163	Create new Socket and connecting to it	socket	com/adobe/marketing/mobile/services/HttpConnectionHandler.java
00012	Read data and put it into a buffer stream	file	epic/mychart/android/library/utilities/i.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java
00183	Get current camera parameters and change the setting.	camera	com/vonage/webrtc/Camera1Session.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://methodistmobileenterprise.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://haiku-push-notifications.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/1062299692154/namespaces/firebase:fetch?key=AIzaSyBk7ZBJ3t3p6rHh3FKp2j4Torwq0qhaGE8 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'about_me_video': 'true', 'amwell_rejoin_visit': 'true', 'amwell_support_number': '{"enabled":true,"content":"346.356.3060"}', 'auto_detect_credit_card': 'true', 'core_facebook_sdk': 'false', 'covid19_landing': '{\n "enabled": false,\n "logo": "https://uatmethodistmobileapi.houstonmethodist.org/images/vuc-hours.png",\n "button2_text": "Close",\n "button1_text": "COVID-19 Update",\n "button1_url": "https://www.houstonmethodist.org/coronavirus/update-for-patients",\n "button2_action": "ok",\n "render": "external",\n "title": "Attention All Patients",\n "content": "Due to the current COVID-19 surge, we have adjusted our Virtual Urgent Care hours. On-demand video visits are now offered daily:\\n 7 a.m. to 11 p.m.\\nWe apologize in advance if wait times are longer than usual.\\n\\n If this is an emergency, please dial 911."\n}', 'dexcare_support_number': '{"enabled": true, "content": "346.356.3060"}', 'dexcare_vuc_offline': 'false', 'emergency_vuc_list_option': '{"enable":false,"render":"external","list_title":"COVID-19 Symptom Checker","list_action":"web","list_content":"https://www.buoyhealth.com/symptom-checker/?configuration=houstonmethodist_02&concern=coronavirus&cta=mymethodist"}', 'fad_profile_comments': 'true', 'image_appointment_url': '{"enabled":true,"render":"external","url":"https://app.blockitnow.com/consumer/houstonmethodistimaging"}', 'insurance_dob_hotfix': 'true', 'main_menu_banner': '{"enabled":true,"title":"COVID-19 Monoclonal Antibody","excerpt":"Houston Methodist has resumed its monoclonal...","border_color":"#FFFFFF","text_alignment":"left","content":"Houston Methodist has resumed its monoclonal antibody infusions with Strovimab, which has shown to be effective against the COVID-19 omicron variant. Due to limited supply, at this time we will only be able to refer patients who are immune compromised or over the age of 65 with a risk factor. This limited supply also means that referrals are not guaranteed even for patients who may qualify.","button_title":"Read Momore","button_action_url":"https://www.houstonmethodist.org/coronavirus/monoclonal-antibody-therapy","button_action_type":"external","secondary_button_title":"","secondary_button_url":"","secondary_button_action_type":""}', 'new_left_menu': 'true', 'onboarding': 'true', 'payment_authorization_banner': '{"enabled":true,"content":"We verify your card by placing a temporary authorization on your account. You may see two payments temporarily. Don’t worry, it’s not an additional charge and it will remove itself in 7-10 business days."}', 'same_day_clinic_appt': 'true', 'vc_location_check_enabled': 'false', 'vuc_latency': '{ "enabled": false, "screen_title": "Longer Wait Times", "screen_message": "Due to the current COVID-19 pandemic, you may experience longer wait times.\\nClick below to learn more or reach a provider by phone.", "button_one_text": "Learn More", "button_one_url": "https://www.houstonmethodist.org/coronavirus/", "button_two_text": "Call Now", "button_two_number": "832-768-7265" }', 'waiting_room_instruction': '{"enable":true,"content":"Please do not leave the waiting room or navigate to another app in order to keep your position in line."}'}, 'state': 'UPDATE', 'templateVersion': '91'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE
Other Common Permissions	7/44	android.permission.CALL_PHONE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, 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

DOMAIN	STATUS	GEOLOCATION
merchant-ui-api.stripe.com	ok	**IP:** 44.235.152.108 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
app.blockitnow.com	ok	**IP:** 35.190.78.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
player.vimeo.com	ok	**IP:** 162.159.128.61 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.opentok.com	ok	**IP:** 168.100.107.128 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.stripe.com	ok	**IP:** 54.68.165.206 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
blobs.griffon.adobe.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
device.griffon.adobe.com	ok	**IP:** 13.224.53.4 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
errors.stripe.com	ok	**IP:** 198.137.150.111 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ichart2.epic.com	ok	**IP:** 199.204.56.101 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
open-scheduling.houstonmethodist.org	ok	**IP:** 206.83.49.108 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.684578 **Longitude:** -95.398766 **View:** Google Map
checkout.link.com	ok	**IP:** 151.101.64.176 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.datacontract.org	ok	**IP:** 207.46.232.160 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
methodistmobileapi.houstonmethodist.org	ok	**IP:** 206.83.49.108 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.684578 **Longitude:** -95.398766 **View:** Google Map
clientsdk.launchdarkly.com	ok	**IP:** 151.101.193.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.houstonmethodistcare.org	ok	No Geolocation information available.
mychart-np.et0922.epichosted.com	ok	**IP:** 170.133.217.249 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** Google Map
m.stripe.com	ok	**IP:** 52.41.92.8 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
methodistmobileenterprise.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
link.co	ok	**IP:** 13.224.53.115 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.epic.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
haiku-push-notifications.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
mobile.launchdarkly.com	ok	**IP:** 54.196.208.134 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
rex.webqa.epic.com	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
www.shareeverywhere.com	ok	**IP:** 199.204.56.202 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
www.houstonmethodist.org	ok	**IP:** 157.55.87.30 **Country:** United States of America **Region:** Texas **City:** San Antonio **Latitude:** 29.424120 **Longitude:** -98.493629 **View:** Google Map
mychart.et0922.epichosted.com	ok	**IP:** 170.133.216.143 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** Google Map
onlinescheudling.houstonmethodist.org	ok	No Geolocation information available.
static.afterpay.com	ok	**IP:** 104.19.176.211 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
clientstream.launchdarkly.com	ok	**IP:** 3.33.235.18 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ichart1.epic.com	ok	**IP:** 204.187.138.40 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	ok	**IP:** 52.216.186.157 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.74.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
stripe.com	ok	**IP:** 54.189.200.54 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.mychart.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
q.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
open-scheduling-widget.houstonmethodist.org	ok	**IP:** 206.83.49.107 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.684578 **Longitude:** -95.398766 **View:** Google Map
altbeacon.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
ecvapi.houstonmethodistcare.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.38.161.73 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	com/stripe/android/core/e.java
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/networking/ApiRequest.java
example@example.com support@stripe.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"Branding_Google_Client_Secret" : "Bj7s1AG-Pfr8bng3hWZl1ofB"
"GOOGLE_API_KEY" : "AIzaSyBk7ZBJ3t3p6rHh3FKp2j4Torwq0qhaGE8"
"access_key" : "1d146377725974998427d20a3be162c3db5604ec"
"com.google.firebase.crashlytics.mapping_file_id" : "4563542841b5448485e52df10e8c94f1"
"credentials" : "Credentials"
"dexcare_api_key" : "android-3d3be662-2221-4b25-b992-e4fdea698cd8"
"firebase_database_url" : "https://methodistmobileenterprise.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBk7ZBJ3t3p6rHh3FKp2j4Torwq0qhaGE8"
"google_crash_reporting_api_key" : "AIzaSyBk7ZBJ3t3p6rHh3FKp2j4Torwq0qhaGE8"
"google_maps_key" : "AIzaSyCuE36X1oImnm8vQ43zccBVRRygwe0_0r4"
"google_places_key" : "AIzaSyCuE36X1oImnm8vQ43zccBVRRygwe0_0r4"
"launchDarklyMobileKey" : "mob-2ddcfc56-0e12-48d8-bd68-e9e9d54e8187"
"mychart_password" : "Password"
"mychart_username" : "Username"
"password" : "Password"
"signature_key" : "8eb012bee620dde5decbed612147d576b5e27340"
"stripe_public_key" : "pk_live_51IJ6CMDXbwgL2Nmj9lMbmay2Q1j62mKbDC69ZroMP8DvDfZlGptLJcRF52sa7ErJqiLzscMX3QxcvyT8JO1WkwnF00roQORFxB"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_clear_disc_webview_cache" : "wp_key_preferences_clear_disc_webview_cache"
"wp_key_preferences_clear_ram_webview_cache" : "wp_key_preferences_clear_ram_webview_cache"
"wp_key_preferences_clear_webview_cache" : "wp_key_preferences_clear_webview_cache"

POSSIBLE SECRETS
"wp_key_preferences_custom_locale" : "wp_key_preferences_custom_locale"
"wp_key_preferences_custom_phone_book" : "wp_preference_custom_phone_book"
"wp_key_preferences_custom_server" : "wp_preference_custom_server"
"wp_key_preferences_custom_server_switch" : "wp_preference_custom_server_switch"
"wp_key_preferences_enable_webview_cache" : "wp_key_preferences_enable_webview_cache"
"wp_key_preferences_health_connect_switch" : "wp_key_preferences_health_connect_switch"
"wp_key_preferences_health_data_debug_switch" : "wp_key_preferences_health_data_debug_switch"
"wp_key_preferences_screenshots" : "wp_preference_screenshots"
"wp_key_preferences_testing_header" : "wp_preferences_testing_header"
"wp_key_preferences_tool_tip" : "wp_key_preferences_tool_tip"
"wp_key_preferences_webivew_cache_header" : "wp_preferences_webview_cache_header"
"wp_login_password" : "Password"
"wp_login_username" : "Username"
"wp_share_everywhere_dismiss_token_button_title" : "Dismiss"
"wp_two_factor_authenticate_code_button" : "Verify"

POSSIBLE SECRETS
"wp_two_factor_authentication_success_accessibility_announcement" : "Success!"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
f8b5b2b5-2b48-48ef-ba72-f11ebebd3e9a
115792089237316195423570985008687907853269984665640564039457584007908834671663
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976l230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
dcb428fea25c40e7b99f81ae5981ee6a
32670510020758816978083085130507043184471273380659243275938904335757337482424

POSSIBLE SECRETS

2c0a9f9dea35f14799cc862258fccea4
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
deca87e736574c5c83c07314051fd93a
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
766354878172a5984fea102e9323a5d3f91cf2f7
9a04f079-9840-4286-ab92-e65be0885f95
55066263022277343669578718895168534326250603453777594175500187360389116729240
48439561293906451759052585252797914202762949526041747995844080717082404635286
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
e2719d58-a985-b3c9-781a-b030af78d30e

POSSIBLE SECRETS

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965808101243442775783767 84
b7b86ef57b18a5c1e2a0d4309d375a58
f35c1d161e65ddc0c06977fa902ebb0c
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
71f8cf7d83deae7b38191cd22946d47b54d59471
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
115792089237316195423570985008687907852837564279074904382605163141518161494337
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
05a1fba0d32e243273c22eeb59f64e00
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
b7aa9702-ab67-42c5-90cd-da22a8b28419

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709168141616373158959998 46
d19f85b6-5337-46a2-894c-94ba72c1b59d
855CF034-1305-481F-8239-3F7F2749C286
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9
115792089210356248762697446949407573530086143415290314195533631308867097853948
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
2624703509579968926862315674456698189185292349110921338781561590092551885473805008902238805397571978665087247673208 7
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
4607e69c-89b9-483b-8cdf-32f3e2ad9287
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: MyMethodist

Score: 4.6666665 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.houstonmethodist.methodistmobile

Developer Details: Houston Methodist, Houston+Methodist, None, http://www.houstonmethodist.org, appsupport@houstonmethodist.org,

Release Date: Feb 4, 2019 **Privacy Policy:** Privacy link

Description:

Quality Health Care at Your Fingertips Accessing Houston Methodist just got easier with the new MyMethodist app. Enjoy 24/7 video visits, securely view MyChart health records and test results, schedule an appointment, find a location and more. AVAILABLE NOW: Houston Methodist Virtual Urgent Care 24/7 access to board-certified providers for non-emergency needs via on-demand video visits. For new and existing patients, no appointment necessary. During your video visit, the telehealth provider will assess your condition, offer a diagnosis and treatment plan, and, if necessary, prescribe medication. Virtual health care visits are ideal for diagnosing and treating common urgent care conditions. Visit houstonmethodist.org/virtual-urgent-care for more information. APP FEATURES: ACCESS YOUR HEALTH RECORDS MyChart: Securely access your Houston Methodist health records, including test and lab results via MyChart. You can also refill prescriptions, communicate with your doctor’s office and more. SEE A DOCTOR Virtual Urgent Care: 24/7 access to board-certified providers for non-emergency needs via on-demand video visits. Our providers are available to see you anytime, even on holidays. Second Opinion: Get secure, convenient and fast online second opinion consultations from Houston Methodist. Our world-class experts review your case, confirm your diagnosis or treatment plan or recommend alternatives. GET CARE Schedule an Appointment: Quickly and conveniently schedule a doctor’s or imaging appointment at one of our convenient locations. Doctor Info: Find your doctor’s information, as well as select a new primary care doctor, another provider or specialist. Plus, read real ratings and reviews from patients just like you. FIND US Find a Location: Find the location nearest you, including emergency care, or get turn-by-turn driving directions to all of our locations. Wayfinding: If you’re at one of our hospital locations, use this feature to navigate to clinic and imaging appointments, dining options, gift shops, ATMs, parking garages and more.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 15:07:04	Generating Hashes	OK
2025-09-01 15:07:04	Extracting APK	OK
2025-09-01 15:07:04	Unzipping	OK

2025-09-01 15:07:04	Parsing APK with androguard	OK
2025-09-01 15:07:05	Extracting APK features using aapt/aapt2	OK
2025-09-01 15:07:05	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 15:07:08	Parsing AndroidManifest.xml	OK
2025-09-01 15:07:08	Extracting Manifest Data	OK
2025-09-01 15:07:08	Manifest Analysis Started	OK
2025-09-01 15:07:17	Reading Network Security config from network_security_config.xml	OK
2025-09-01 15:07:17	Parsing Network Security config	OK
2025-09-01 15:07:17	Performing Static Analysis on: MyMethodist (org.houstonmethodist.methodistmobile)	OK
2025-09-01 15:07:19	Fetching Details from Play Store: org.houstonmethodist.methodistmobile	OK
2025-09-01 15:07:21	Checking for Malware Permissions	OK

2025-09-01 15:07:21	Fetching icon path	OK
2025-09-01 15:07:21	Library Binary Analysis Started	OK
2025-09-01 15:07:21	Reading Code Signing Certificate	OK
2025-09-01 15:07:21	Running APKiD 2.1.5	OK
2025-09-01 15:07:24	Detecting Trackers	OK
2025-09-01 15:07:31	Decompiling APK to Java with JADX	OK
2025-09-01 15:07:47	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 15:07:47	Decompiling classes6.dex with JADX	OK
2025-09-01 15:07:49	Decompiling classes8.dex with JADX	OK
2025-09-01 15:07:57	Decompiling classes2.dex with JADX	OK
2025-09-01 15:08:00	Decompiling classes4.dex with JADX	OK

2025-09-01 15:08:08	Decompiling classes.dex with JADX	OK
2025-09-01 15:08:17	Decompiling classes3.dex with JADX	OK
2025-09-01 15:08:21	Decompiling classes5.dex with JADX	OK
2025-09-01 15:08:26	Decompiling classes7.dex with JADX	OK
2025-09-01 15:08:34	Decompiling classes6.dex with JADX	OK
2025-09-01 15:08:36	Decompiling classes8.dex with JADX	OK
2025-09-01 15:08:43	Decompiling classes2.dex with JADX	OK
2025-09-01 15:08:46	Decompiling classes4.dex with JADX	OK
2025-09-01 15:08:54	Decompiling classes.dex with JADX	OK
2025-09-01 15:09:03	Decompiling classes3.dex with JADX	OK
2025-09-01 15:09:08	Decompiling classes5.dex with JADX	OK

2025-09-01 15:09:13	Decompiling classes7.dex with JADX	OK
2025-09-01 15:09:20	Converting DEX to Smali	OK
2025-09-01 15:09:20	Code Analysis Started on - java_source	OK
2025-09-01 15:09:30	Android SBOM Analysis Completed	OK
2025-09-01 15:09:37	Android SAST Completed	OK
2025-09-01 15:09:37	Android API Analysis Started	OK
2025-09-01 15:09:45	Android API Analysis Completed	OK
2025-09-01 15:09:45	Android Permission Mapping Started	OK
2025-09-01 15:09:59	Android Permission Mapping Completed	OK
2025-09-01 15:09:59	Android Behaviour Analysis Started	OK
2025-09-01 15:10:09	Android Behaviour Analysis Completed	OK

2025-09-01 15:10:09	Extracting Emails and URLs from Source Code	OK
2025-09-01 15:10:20	Email and URL Extraction Completed	OK
2025-09-01 15:10:20	Extracting String data from APK	OK
2025-09-01 15:10:20	Extracting String data from Code	OK
2025-09-01 15:10:20	Extracting String values and entropies from Code	OK
2025-09-01 15:10:28	Performing Malware check on extracted domains	OK
2025-09-01 15:10:32	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.