MOBSF

ANDROID STATIC ANALYSIS REPORT

MyHealth (10.3)

File Name:	org.stanfordhealthcare.myhealth_10308.apk
Package Name:	org.stanfordhealthcare.myhealth
Scan Date:	Sept. 1, 2025, 4:57 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	18	3	2	2

FILE INFORMATION

File Name: org.stanfordhealthcare.myhealth_10308.apk
Size: 28.02MB
MD5: 14da178ade5a578fa5b008365073cb11
SHA1: 4340817e04209703affe0d6448eba0b808a22326
SHA256: bf4e296e64ced22d4efdb868c93fb05dcf585a0eb9c036835ecd835e287e01db

APP INFORMATION

App Name: MyHealth
Package Name: org.stanfordhealthcare.myhealth
Main Activity: epic.mychart.prelogin.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 10.3

Android Version Code: 10308

APP COMPONENTS

Activities: 99
Services: 21
Receivers: 12
Providers: 3
Exported Activities: 1
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Palo Alto, O=Stanford Health Care, OU=ITS
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-10-30 22:02:37+00:00
Valid To: 2040-10-23 22:02:37+00:00
Issuer: C=US, ST=California, L=Palo Alto, O=Stanford Health Care, OU=ITS
Serial Number: 0x6c581f1b
Hash Algorithm: sha256
md5: 8daffbcb76e2716c101e6e5ea5998e9c
sha1: 164c3ebeac9059bc4267a887f27655da144e52ac
sha256: f8508413eb5596234316937060e013829389a89721f5afa6f38b5456f69c7684
sha512: bd98f68b1497ca0b45ee1c8c01a1df9363396fea4a035a865ebef02a0386ebac3faad6ca2633fc6412cf5b5f92f3f25edfacb8d022a3724f561d4bf821843429
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3319449c3aa19a63c9e033ce7624cb50acbd94771c22bb3287c6e1de77479549
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
epic.mychart.MyChart	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
org.stanfordhealthcare.myhealth.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
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.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_LOCATION	unknown	Unknown permission	Unknown permission from android reference

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.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
org.stanfordhealthcare.myhealth.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>14da178ade5a578fa5b008365073cb11.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>
<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
SIM operator check
possible VM 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>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>

<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.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS 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.prelogin.SplashActivity	Schemes: epicmychart://, Hosts: orgselect,
org.shc.myhealth.activities.SHCLoginActivity	Schemes: https://, Hosts: myshc.org, Paths: /qnr, Path Patterns: /econsent,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

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: 8 | 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.shc.myhealth.activities.SHCLoginActivity) 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	Service (epic.mychart.googlefit.GoogleFitSyncService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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: **2** | WARNING: **8** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/arubanetworks/meridian/internal/util/DependencyCheck.java com/arubanetworks/meridian/log/AndroidStandardLogAdapter.java com/arubanetworks/meridian/maprender/GLTextureView.java com/arubanetworks/meridian/util/Strings.java com/vidyo/lmi/BatteryManager.java com/vidyo/lmi/LocationManager.java com/vidyo/lmi/ScreenManager.java com/vidyo/lmi/ui/Window.java epic/mychart/appointments/AppointmentsListFragment.java epic/mychart/appointments/FutureAppointmentFragment.java epic/mychart/billing/BillPaymentActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				epic/mychart/customobjects/WPSSLSocketFactory.java epic/mychart/customviews/SHCInstructionsTextView.java epic/mychart/customviews/UnsupportedFileViewerActivity.java epic/mychart/geofence/SHCGeofencingManager.java epic/mychart/healthadvisories2013/HealthAdvisoryMarkCompleteActivity.java epic/mychart/healthsummary/ImmunizationsContainerFragment.java epic/mychart/infectioncontrol/CovidStatusFragment.java epic/mychart/insurance/TiffViewerWebView.java epic/mychart/medications/SHCSelectPickupPharmacyActivity.java epic/mychart/medications/UpdatePickupPharmacyPagesFlow.java epic/mychart/medications/renewals/MedicationsRenewalActivity.java epic/mychart/medications/renewals/MedicationsRenewalPagesFlow.java epic/mychart/messages/ComposeActivity.java epic/mychart/messages/MessageDetailsFragment.java epic/mychart/messages/MessageDetailsFragmentViewModel.java epic/mychart/open/WPBaseFeatureType.java epic/mychart/open/WPOpen.java epic/mychart/prelogin/SplashActivity.java epic/mychart/prelogin/SplashActivityViewModel.java epic/mychart/questionnaires/PreLoginQuestionnairesActivity.java epic/mychart/telemedicine/VideoVisitManager.java epic/mychart/telemedicine/vidyo/ClosedCaptionToken.java epic/mychart/telemedicine/vidyo/MyHealthVid

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yoConnectionInfo.java epic/mychart/telemedicine/vidyo/VideoFrameFragment.java epic/mychart/telemedicine/vidyo/VidyoClosedCaptionClient.java epic/mychart/telemedicine/vidyo/VidyoConnectorManager.java epic/mychart/telemedicine/vidyo/VidyoVisitActivity.java epic/mychart/testresults/TestResultDetailsFragment.java epic/mychart/trackmyhealth/AddFlowsheetReadingsFragment.java epic/mychart/utilities/DataConnector.java epic/mychart/utilities/GsonUtil.java epic/mychart/utilities/SHCUtil.java epic/mychart/utilities/WPUtil.java epic/mychart/utilities/WPXML.java org/conscrypt/Platform.java org/conscrypt/ct/CTVerifier.java org/healthcare/stanford/blescan/BeaconManager.java org/healthcare/stanford/blescan/BluetoothScanBroadcastReceiver.java org/healthcare/stanford/blescan/OnExitBeaconService.java org/healthcare/stanford/blescan/ScanService.java org/shc/myhealth/SHC_FcmListenerService.java org/shc/myhealth/activities/SHCLoginActivity.java org/shc/myhealth/alertcenter/AlertCenterDataManager.java org/shc/myhealth/alertcenter/AlertCenterEnabledTitledActivity.java org/shc/myhealth/alertcenter/AlertCenterEnabledTitledFragment.java org/shc/myhealth/alertcenter/AlertCenterEventsActivity.java org/shc/myhealth/alertcenter/PipelineEventVie

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	wModel.java org/shc/myhealth/alertcenter/PipelineEventsRecycleAdapter.java org/shc/myhealth/arrival/MeridianUtils.java org/shc/myhealth/billing/ExternalPaymentWebView.java org/shc/myhealth/billing/ExternalPaymentWebViewFragment.java org/shc/myhealth/customviews/SHCNavigationButtonView.java org/shc/myhealth/echeckin/ECheckinActivity.java org/shc/myhealth/echeckin/ECheckinPagesFlow.java org/shc/myhealth/echeckin/pages/ECheckinAllergiesPage.java org/shc/myhealth/echeckin/pages/ECheckinInsurancePage.java org/shc/myhealth/echeckin/pages/ESignDocumentPage.java org/shc/myhealth/echeckin/pages/QuestionnaireWebView.java org/shc/myhealth/esignature/CustomWebView.java org/shc/myhealth/fragments/SHCDialogFragment.java org/shc/myhealth/futureappointmentviews/SHCTrackerView.java org/shc/myhealth/healthsummary/AllergyActivity.java org/shc/myhealth/inpatient/careteam/CareTeamListAdapter.java org/shc/myhealth/maps/LocationAdapter.java org/shc/myhealth/maps/PlacemarkDownloader.java org/shc/myhealth/meridianmodel/FloorMaps.java org/shc/myhealth/meridianmodel/MeridianModel.java org/shc/myhealth/messagedialog/SHCMessageDialog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Dialog.java org/shc/myhealth/messages/SHCOrionAttachmentContainer.java org/shc/myhealth/notification/MyHealthNotification.java org/shc/myhealth/notification/NotificationParcelCreator.java org/shc/myhealth/orderedtests/OrderedTestsDetailsFragment.java org/shc/myhealth/orderedtests/OrderedTestsListAdapter.java org/shc/myhealth/orderedtests/OrderedTestsViewModel.java org/shc/myhealth/prelogin/accountmanagement/SHCForgotIdSendReminderPage.java org/shc/myhealth/prelogin/accountmanagement/SHCNewAccountCreditHistoryPagesFlow.java org/shc/myhealth/quickschedule/QuickScheduleWebViewFragment.java org/shc/myhealth/scheduling/AppointmentProviderClinicsAdapter.java org/shc/myhealth/scheduling/AppointmentProviderWorkflowPage.java org/shc/myhealth/scheduling/DynamicPageAdapter.java org/shc/myhealth/scheduling/ProviderDepartmentHelper.java org/shc/myhealth/scheduling/ScheduleAppointmentActivity.java org/shc/myhealth/scheduling/ScheduleAppointmentPagesFlow.java org/shc/myhealth/scheduling/SchedulingQuestionnaireAdapter.java org/shc/myhealth/scheduling/TicketSchedulingActivity.java org/shc/myhealth/scheduling/TimeSlotsFilterActivity.java org/shc/myhealth/scheduling/TimeSlotsWorkflowPage.java org/shc/myhealth/servers/SHCServers.java org/shc/myhealth/servers/SHCSettingsActivity.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/shc/myhealth/servers/SHCSettingsActivity.java org/shc/myhealth/servers/SHCStorageUtil.java org/shc/myhealth/service/LogsUploadService.java org/shc/myhealth/utilities/ImageDownloader.java org/shc/myhealth/utilities/SHCDeviceRegistration.java org/shc/myhealth/utilities/SHCHttpUtil.java org/shc/myhealth/wayfinding/WayfindingActivity.java org/shc/myhealth/workflowframework/WorkflowPagesFlow.java org/slf4j/helpers/Util.java org/stanfordhealthcare/myhealth/orionapi/api/OrionApi.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java org/stanfordhealthcare/myhealth/orionapi/model/OrionModel.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
				com/arubanetworks/meridian/BuildConfig.java com/arubanetworks/meridian/editor/Placemark.java com/arubanetworks/meridian/locationsharing/UploadLocationService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/arubanetworks/meridian/locationsharing/UserLava com/arubanetworks/meridian/maps/mapSheet/Link.java epic/mychart/appointments/FutureAppointmentFragment.java epic/mychart/appointments/WebSchedulingActivity.java epic/mychart/general/DeepLinkManager.java epic/mychart/googlefit/GoogleFitDataFetcher.java epic/mychart/googlefit/GoogleFitJobScheduler.java epic/mychart/healthadvisories2013/HealthAdvisoryMarkCompleteActivity.java epic/mychart/messages/WebMessageTasksActivity.java epic/mychart/telemedicine/StreamingStatusService.java epic/mychart/telemedicine/vidyo/MyHealthVidyoConnectionInfo.java epic/mychart/telemedicine/vidyo/VidyoVisitActivity.java epic/mychart/utilities/Constants.java epic/mychart/utilities/DataConnector.java epic/mychart/utilities/Session.java epic/mychart/utilities/Storage.java epic/mychart/webapp/Parameter.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java org/java_websocket/drafts/Draft_6455.java org/shc/myhealth/activities/SHCLoginActivity.java org/shc/myhealth/inpatient/patientrequests/GeneralRequestItemFragmentArgs.java org/shc/myhealth/inpatient/patientrequests/GeneralRequestsFragmentDirections.java org/shc/myhealth/notification/MyHealthNotification.java org/shc/myhealth/utilities/BiometricAuthentica

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tor.java org/stanfordhealthcare/myhealth/orionapi/api/OrionAPIHeaderKey.java
				org/stanfordhealthcare/myhealth/orionapi/api/OrionApi.java org/stanfordhealthcare/myhealth/orionapi/model/appointment_scheduling/OrionDecisionTreeResponse.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 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	epic/mychart/customobjects/ExternalFile.java epic/mychart/utilities/FileUtil.java epic/mychart/utilities/WPAndroidAPI.java epic/mychart/utilities/WPDeviceUtil.java org/shc/myhealth/SHCApplication.java org/shc/myhealth/model/MyHealthDebugLog.java
5	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	org/shc/myhealth/echeckin/pages/ESignDocumentPage.java org/shc/myhealth/echeckin/pages/QuestionnaireWebView.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java
6	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	epic/mychart/utilities/FileUtil.java epic/mychart/utilities/Storage.java org/shc/myhealth/utilities/SHCMiscUtilities.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/arubanetworks/meridian/internal/util/Sec.java com/arubanetworks/meridian/requests/MapImageRequest.java epic/mychart/utilities/Crypto.java org/java_websocket/drafts/Draft_6455.java
10	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	org/shc/myhealth/utilities/BiometricAuthenticator.java
11	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	epic/mychart/utilities/WPAndroidAPI.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/arubanetworks/meridian/internal/util/Sec.java epic/mychart/utilities/WPUtil.java
13	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/arubanetworks/meridian/locationsharing/b.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/arubanetworks/meridian/maps/MapSheetFragment.java com/arubanetworks/meridian/maps/mapSheet/PlacemarkBottomSheet.java epic/mychart/customactivities/JavaScriptWebViewActivity.java epic/mychart/customactivities/TitledMyChartActivity.java epic/mychart/customactivities/TitledWebViewActivity.java epic/mychart/general/DeepLinkManager.java epic/mychart/medications/MedicationBodyActivity.java epic/mychart/messages/BrowserSpan.java epic/mychart/messages/ComposeActivity.java epic/mychart/messages/SHCMessageHelper.java epic/mychart/messages/WebMessageTasksActivity.java epic/mychart/prelogin/PreLoginUtil.java epic/mychart/springboard/MainFragment.java epic/mychart/springboard/WPCustomFeature.java epic/mychart/testresults/TestDetailImagesView.java epic/mychart/testresults/TestResultDetailsFragment.java epic/mychart/utilities/SHCUtil.java epic/mychart/utilities/WPUtil.java epic/mychart/utilities/WPWeb.java org/shc/myhealth/SHCLogEventWebViewClient.java org/shc/myhealth/SHCVersionActivity.java org/shc/myhealth/activities/SHCLoginActivity.java org/shc/myhealth/activities/SHCNavigationDrawerActivity.java org/shc/myhealth/billing/BillingWebViewFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/shc/myhealth/echeckin/pages/NewInsurancePage.java org/shc/myhealth/echeckin/pages/QuestionnaireWebView.java org/shc/myhealth/ed/transitioncare/TransitionCareRootFragment.java org/shc/myhealth/fragments/AemWebViewFragment.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java org/shc/myhealth/fragments/WebViewDisclaimerFragment.java org/shc/myhealth/inpatient/careteam/CareTeamFragment.java org/shc/myhealth/inpatient/healthmetrics/HealthMetricDetailsActivity.java org/shc/myhealth/inpatient/healthmetrics/HealthMetricsFragment.java org/shc/myhealth/inpatient/hospitalinfo/HospitalInfoFragment.java org/shc/myhealth/inpatient/medications/InpatientMedicineDetailsFragment.java org/shc/myhealth/inpatient/patientgoals/goalviews/PainInfoView.java org/shc/myhealth/inpatient/patientrequests/ServiceRequestItemFragment.java org/shc/myhealth/orderedtests/OrderedTestsDetailsFragment.java org/shc/myhealth/patienteducation/PatientEducationLandingFragment.java org/shc/myhealth/patienteducation/PatientEducationPointFragment.java org/shc/myhealth/permissions/PermissionsUtility.java org/shc/myhealth/procedures/ProcedureDetailsActivity.java org/shc/myhealth/procedures/ProcedureVideoFragment.java org/shc/myhealth/scheduling/TimeSlotsAdapter.java
00013	Read file and put it into a stream	file	com/arubanetworks/meridian/location/MeridianLocationService.java com/arubanetworks/meridian/triggers/TriggersCache.java epic/mychart/customobjects/ExternalFile.java epic/mychart/customviews/PhotoViewerActivity.java epic/mychart/customviews/UnsupportedFileViewerActivity.java epic/mychart/messages/ComposeActivity.java epic/mychart/utilities/Storage.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java org/shc/myhealth/arrival/ArrivalManager.java org/shc/myhealth/notification/NotificationStore.java org/shc/myhealth/service/LogsUploadService.java org/shc/myhealth/utilities/AWSRequestBuilder.java org/shc/myhealth/utilities/SHCMiscUtilities.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	epic/mychart/appointments/AppointmentsListFragment.java epic/mychart/appointments/FutureAppointmentFragment.java epic/mychart/billing/AddNewCardActivity.java epic/mychart/billing/BillPaymentActivity.java epic/mychart/billing/PaymentConfirmationActivity.java epic/mychart/healthadvisories2013/HealthAdvisoryMarkCompleteActivity.java epic/mychart/medications/MedRefillActivity.java epic/mychart/medications/MedicationBodyActivity.java epic/mychart/medications/renewals/MedicationsRenewalActivity.java epic/mychart/messages/ComposeActivity.java epic/mychart/telemedicine/StreamingStatusService.java epic/mychart/testresults/TestResultDetailsActivity.java epic/mychart/testresults/TestResultTrendsActivity.java org/shc/myhealth/activities/SHCLoginActivity.java org/shc/myhealth/documents/PreLoginESignDocumentActivity.java org/shc/myhealth/echeckin/ECheckinActivity.java org/shc/myhealth/echeckin/ESignDocumentActivity.java org/shc/myhealth/procedures/ProcedureDetailsActivity.java
00022	Open a file from given absolute path of the file	file	com/arubanetworks/meridian/maprender/GLTextureMapView.java com/arubanetworks/meridian/maprender/TextureProviderFile.java com/arubanetworks/meridian/maps/MapView.java epic/mychart/customviews/VideoPlayerActivity.java epic/mychart/messages/MessageDetailsFragment.java epic/mychart/telemedicine/vidyo/VidyoVisitActivity.java epic/mychart/utilities/Storage.java org/shc/myhealth/activities/MyHealthDebugLogActivity.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java org/shc/myhealth/messages/SHCOrionAttachmentContainer.java org/shc/myhealth/servers/SHCStorageUtil.java org/shc/myhealth/service/LogsUploadService.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/googlefit/GoogleFitService.java org/shc/myhealth/alertcenter/PipelineEventViewModel.java

RULE ID	BEHAVIOUR	LABEL	FILES
00202	Make a phone call	control	com/arubanetworks/meridian/maps/mapSheet/PlacemarkBottomSheet.java epic/mychart/utilities/SHCUtil.java epic/mychart/utilities/WPUtil.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java org/shc/myhealth/inpatient/patientrequests/ServiceRequestItemFragment.java org/shc/myhealth/patienteducation/PatientEducationPointFragment.java
00203	Put a phone number into an intent	control	com/arubanetworks/meridian/maps/mapSheet/PlacemarkBottomSheet.java epic/mychart/utilities/SHCUtil.java epic/mychart/utilities/WPUtil.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java org/shc/myhealth/inpatient/patientrequests/ServiceRequestItemFragment.java org/shc/myhealth/patienteducation/PatientEducationPointFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/arubanetworks/meridian/maps/MapSheetFragment.java com/arubanetworks/meridian/maps/mapSheet/PlacemarkBottomSheet.java epic/mychart/springboard/MainFragment.java epic/mychart/utilities/SHCUtil.java epic/mychart/utilities/WPUtil.java org/shc/myhealth/activities/SHCLoginActivity.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java org/shc/myhealth/inpatient/patientrequests/ServiceRequestItemFragment.java org/shc/myhealth/patienteducation/PatientEducationPointFragment.java org/shc/myhealth/permissions/PermissionsUtility.java
00108	Read the input stream from given URL	network command	epic/mychart/customobjects/WPCallInformation.java epic/mychart/googlefit/GoogleFitDataFetcher.java org/shc/myhealth/SHCCustomFont.java org/shc/myhealth/SHCVersionUtil.java org/shc/myhealth/api/MeridianConnectionAsyncTask.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	epic/mychart/googlefit/GoogleFitDataFetcher.java epic/mychart/utilities/DataConnector.java org/shc/myhealth/api/MeridianConnectionAsyncTask.java org/shc/myhealth/service/LogsUploadService.java org/shc/myhealth/utilities/SHCHttpUtil.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java
00109	Connect to a URL and get the response code	network command	epic/mychart/googlefit/GoogleFitDataFetcher.java epic/mychart/telemedicine/VideoVisitManager.java org/shc/myhealth/SHCCustomFont.java org/shc/myhealth/SHCVersionUtil.java org/shc/myhealth/api/MeridianConnectionAsyncTask.java org/shc/myhealth/service/LogsUploadService.java org/shc/myhealth/utilities/SHCHttpUtil.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java
00153	Send binary data over HTTP	http	epic/mychart/utilities/DataConnector.java org/shc/myhealth/service/LogsUploadService.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/java_websocket/client/WebSocketClient.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java org/java_websocket/SSLSocketChannel2.java org/java_websocket/client/WebSocketClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	epic/mychart/googlefit/GoogleFitDataFetcher.java epic/mychart/telemedicine/VideoVisitManager.java epic/mychart/utilities/DataConnector.java org/shc/myhealth/SHCCustomFont.java org/shc/myhealth/SHCVersionUtil.java org/shc/myhealth/api/MeridianConnectionAsyncTask.java org/shc/myhealth/utilities/SHCHttpUtil.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java
00102	Set the phone speaker on	command	com/vidyo/lmi/audio/AudioCentral.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	org/shc/myhealth/messages/SHCOrionAttachmentContainer.java
00123	Save the response to JSON after connecting to the remote server	network command	epic/mychart/googlefit/GoogleFitDataFetcher.java
00030	Connect to the remote server through the given URL	network	epic/mychart/googlefit/GoogleFitDataFetcher.java epic/mychart/utilities/DataConnector.java
00094	Connect to a URL and read data from it	command network	epic/mychart/googlefit/GoogleFitDataFetcher.java org/shc/myhealth/SHCCustomFont.java org/shc/myhealth/SHCVersionUtil.java org/shc/myhealth/api/MeridianConnectionAsyncTask.java org/stanfordhealthcare/myhealth/orionapi/api/OrionConnectionAsyncTask.java
00005	Get absolute path of file and put it to JSON object	file	epic/mychart/telemedicine/vidyo/VidyoVisitActivity.java org/shc/myhealth/fragments/MyHealthWebViewFragment.java
00012	Read data and put it into a buffer stream	file	org/conscrypt/DefaultSSLContextImpl.java org/shc/myhealth/utilities/SHCMiscUtilities.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/arubanetworks/meridian/location/MeridianLocationService.java org/shc/myhealth/arrival/ArrivalManager.java
00036	Get resource file from res/raw directory	reflection	com/arubanetworks/meridian/Meridian.java org/shc/myhealth/permissions/PermissionsUtility.java
00072	Write HTTP input stream into a file	command network file	org/shc/myhealth/SHCCustomFont.java
00004	Get filename and put it to JSON object	file collection	epic/mychart/telemedicine/vidyo/VidyoVisitActivity.java org/shc/myhealth/arrival/ArrivalManager.java
00125	Check if the given file path exist	file	epic/mychart/utilities/WPUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://stanford-health-care-myhealth-3933c.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/642142923121/namespaces/firebase:fetch?key=AIzaSyC6EEv7IiICuy-6c3pmbry0ffJL8Wa4Vfs. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.VIBRATE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_BACKGROUND_LOCATION, 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
stanford-health-care-myhealth-3933c.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
stagemychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
pocmychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
myhealthmobile.s3.amazonaws.com	ok	**IP:** 52.216.54.193 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
healthed.stanfordhealthcare.org	ok	**IP:** 54.165.36.126 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
edit.meridianapps.com	ok	**IP:** 35.227.232.70 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.google-analytics.com	ok	**IP:** 142.250.74.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
myhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.172 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
portal.vidyo.com	ok	No Geolocation information available.
tags-direct.meridianapps.com	ok	**IP:** 104.197.193.115 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
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:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
myhealthmobile.stanfordhealthcare.org	ok	**IP:** 18.155.173.107 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
pocmyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
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
www.healthwise.net	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
dev-edit.meridianapps.com	ok	**IP:** 35.244.235.26 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **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
dev-tags-direct.meridianapps.com	ok	**IP:** 34.82.179.136 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** Google Map
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
staging-edit.meridianapps.com	ok	**IP:** 34.149.46.88 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
uatmychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.230 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
www.stanfordhospital.org	ok	**IP:** 3.233.235.201 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.74.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
epic-wbs-test.stanfordmed.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
genmychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
supdmyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.151 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
stagemyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
genmyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.203 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
uatmyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.229 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
supdmychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.153 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
edit-eu.meridianapps.com	ok	**IP:** 34.110.148.56 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mychart.stanfordhealthcare.org	ok	**IP:** 96.47.58.173 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tags-eu-direct.meridianapps.com	ok	**IP:** 35.241.169.121 **Country:** Belgium **Region:** Brussels Hoofdstedelijk Gewest **City:** Brussels **Latitude:** 50.850449 **Longitude:** 4.348780 **View:** Google Map
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
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
www.googleapis.com	ok	**IP:** 142.250.74.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stanfordhealthcare.org	ok	**IP:** 3.233.235.201 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
staging-tags-direct.meridianapps.com	ok	**IP:** 35.192.202.94 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
mobmyhealth.stanfordhealthcare.org	ok	**IP:** 96.47.58.174 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
shc-myhealthmobile-bucket-prod-381491994404-us-west-2.s3.us-west-2.amazonaws.com	ok	**IP:** 52.92.161.226 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Display		https://reports.exodus-privacy.eu.org/trackers/188

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://stanford-health-care-myhealth-3933c.firebaseio.com"
"google_api_key" : "AIzaSyC6EEv7IiICuy-6c3pmbry0ffJL8Wa4Vfs"
"google_crash_reporting_api_key" : "AIzaSyC6EEv7IiICuy-6c3pmbry0ffJL8Wa4Vfs"
"login_password" : "Password"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
eed03e861ea54e999175e7281ceabe6dd8f05a6b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
2BBWhSkQ9alML8PajNGVixxCUpbw
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
token=UU2UaMsga+94EcW79SiiQPgOKOfez2t9aspNNDSz8p7MJLTY0f9P47VV55mhjbPReceTQKWuMd6jQd2ZxdbUZQj4QfIBJ/TP1x3zwGpbmImlxtQ8m5OEvNXNYCAODFbG
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
edf6b369-2528-48bb-91b5-65bb4422a2c8
24ZZRNrnBszv1Y67qfUUaSbAmisOF4uojeQ21OryW8ajA
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
24Lw6wbhptVgUtAyQcDvu58WpU4bpaNslyyKmdGteh8AQ
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
b208845d-5183-4668-b43a-06c975b59e77
e2514491d9e2456f8808fb177ef54bcb
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
token=L20CBzNY7qphnWzSt3q5NXS+L0jVbPSJhOqdWHTpKmGjrAzAoEzHRpTf9XmWhvk1NDdWooZEDLZHc13aNPaUdK4zk+VQdgwsrq1glRTgje/Z+TOCSd68fQ8I6vp8Yaol
3ff239b737004656a15a7de75a3bcc26
3071c8717539de5d5353f4c8cd59a032
token=vsCc8Mkkcrb+l0b4PEpsrWWa96PUOOKxCw6Pi+hGwmm0SPKTKI7zQM82433eYqARHL7gerbf19vdALdEgkEyF9oVnN29tLBu9y+8VxrJhUOS1EQ3+D9TfPqyGI0+789A
7d73d21f1bd82c9e5268b6dcf9fde2cb
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
acfa2bdc592f268de7e8cb

PLAYSTORE INFORMATION

Title: Stanford Health Care MyHealth

Score: 4.5 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.stanfordhealthcare.myhealth

Developer Details: Stanford Health Care, Stanford+Health+Care, None, http://www.stanfordhealthcare.org, HelpDesk3-3333@stanfordhealthcare.org,

Release Date: Dec 17, 2015 **Privacy Policy:** Privacy link

Description:

Accessing your personal health information has never been easier. The MyHealth mobile app from Stanford Health Care puts your personal information at your fingertips to make managing your health care simple, quick, and completely confidential. With the Stanford Health Care MyHealth app you can: 1. Schedule your in-person appointments or video visits, and eCheck-in for appointments 2. Communicate with your care team 3. View test results and manage medications 4. Inside our buildings, follow step by step directions to your appointment location 5. Review and pay bills 6. Get up to date health information during a stay at the hospital and more...

SCAN LOGS

Timestamp	Event	Error
2025-09-01 16:57:32	Generating Hashes	OK
2025-09-01 16:57:32	Extracting APK	OK
2025-09-01 16:57:32	Unzipping	OK
2025-09-01 16:57:32	Parsing APK with androguard	OK
2025-09-01 16:57:33	Extracting APK features using aapt/aapt2	OK
2025-09-01 16:57:33	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 16:57:35	Parsing AndroidManifest.xml	OK

2025-09-01 16:57:35	Extracting Manifest Data	OK
2025-09-01 16:57:35	Manifest Analysis Started	OK
2025-09-01 16:57:36	Reading Network Security config from network_security_config.xml	OK
2025-09-01 16:57:36	Parsing Network Security config	OK
2025-09-01 16:57:36	Performing Static Analysis on: MyHealth (org.stanfordhealthcare.myhealth)	OK
2025-09-01 16:57:37	Fetching Details from Play Store: org.stanfordhealthcare.myhealth	OK
2025-09-01 16:57:39	Checking for Malware Permissions	OK
2025-09-01 16:57:39	Fetching icon path	OK
2025-09-01 16:57:39	Library Binary Analysis Started	OK
2025-09-01 16:57:39	Reading Code Signing Certificate	OK
2025-09-01 16:57:39	Running APKiD 2.1.5	OK

2025-09-01 16:57:41	Detecting Trackers	OK
2025-09-01 16:57:44	Decompiling APK to Java with JADX	OK
2025-09-01 16:58:29	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 16:58:29	Decompiling classes2.dex with JADX	OK
2025-09-01 16:58:33	Decompiling classes.dex with JADX	OK
2025-09-01 16:58:42	Decompiling with JADX failed for classes.dex	OK
2025-09-01 16:58:43	Decompiling classes3.dex with JADX	OK
2025-09-01 16:58:52	Decompiling classes2.dex with JADX	OK
2025-09-01 16:58:56	Decompiling classes.dex with JADX	OK
2025-09-01 16:59:04	Decompiling classes3.dex with JADX	OK
2025-09-01 16:59:14	Some DEX files failed to decompile	OK

2025-09-01 16:59:14	Converting DEX to Smali	OK
2025-09-01 16:59:14	Code Analysis Started on - java_source	OK
2025-09-01 16:59:16	Android SBOM Analysis Completed	OK
2025-09-01 16:59:21	Android SAST Completed	OK
2025-09-01 16:59:21	Android API Analysis Started	OK
2025-09-01 16:59:25	Android API Analysis Completed	OK
2025-09-01 16:59:25	Android Permission Mapping Started	OK
2025-09-01 16:59:30	Android Permission Mapping Completed	OK
2025-09-01 16:59:31	Android Behaviour Analysis Started	OK
2025-09-01 16:59:36	Android Behaviour Analysis Completed	OK
2025-09-01 16:59:36	Extracting Emails and URLs from Source Code	OK

2025-09-01 16:59:38	Email and URL Extraction Completed	OK
2025-09-01 16:59:38	Extracting String data from APK	OK
2025-09-01 16:59:38	Extracting String data from Code	OK
2025-09-01 16:59:38	Extracting String values and entropies from Code	OK
2025-09-01 16:59:42	Performing Malware check on extracted domains	OK
2025-09-01 16:59:48	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.