MOBSF

ANDROID STATIC ANALYSIS REPORT

Sanford (3.12.0)

File Name:	org.sanfordhealth.patient_39766.apk
Package Name:	org.sanfordhealth.patient
Scan Date:	Sept. 1, 2025, 4:53 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	24	4	1	1

FILE INFORMATION

File Name: org.sanfordhealth.patient_39766.apk
Size: 45.24MB
MD5: 2b23252c4129d6070f2182d359c3630f
SHA1: 30837ea771695bedfbbfa6075add13a5b1925f7a
SHA256: 5a44404fe28414d722b66a97b324fca1c2724ebfdab93faef6b4fcd7fe9d2345

APP INFORMATION

App Name: Sanford
Package Name: org.sanfordhealth.patient
Main Activity: org.sanfordhealth.patient.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 3.12.0

Android Version Code: 39766

APP COMPONENTS

Activities: 102
Services: 27
Receivers: 17
Providers: 7
Exported Activities: 6
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=SD, L=Sioux Falls, O=Sanford Health, OU=Sanford Health, CN=Sanford Health
Signature Algorithm: dsa
Valid From: 2013-04-09 20:42:20+00:00
Valid To: 2287-01-23 20:42:20+00:00
Issuer: C=US, ST=SD, L=Sioux Falls, O=Sanford Health, OU=Sanford Health, CN=Sanford Health
Serial Number: 0x51647d2c
Hash Algorithm: sha1
md5: dbb83712ad6c07477c0d01878a2689d9
sha1: 4394de3dda37e6d8b5fb9f677745b5f5f660e08f
sha256: 7de2a8775abd8fe8aa951361c78847b4a14f063e9ca254f8485cd1e8cf798a19
sha512: 6a1be581c0d602238de1c8e720ad34e2cb821c48e0f8c93d82e1d88d653b6bee2fa5ec4b22ebf18630e6b6599f15f010798e65e762624fbe4a73acc1fe0a823a
PublicKey Algorithm: dsa
Bit Size: 1024
Fingerprint: 32966f49868f0cbed308cc802c5ff9ba52eae3df6e1fbf9384bba31ea80474de
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
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_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
org.sanfordhealth.patient.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>2b23252c4129d6070f2182d359c3630f.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.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>

FILE	DETAILS
classes3.dex	<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>
classes4.dex	<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>

FILE	DETAILS
classes5.dex	<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 possible Build.SERIAL check Build.TAGS check SIM operator check network operator name 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>

FILE	DETAILS
classes6.dex	<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 possible Build.SERIAL check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.sanfordhealth.patient.DeepLinkActivity	Schemes: org.sanfordhealth.patient://,
org.sanfordhealth.patient.AppLinkActivity	Schemes: https://, Hosts: www.mysanfordchart.org, Path Prefixes: /MyChart, /mychart,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 13 | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/wp_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.
3	Activity (org.sanfordhealth.patient.DeepLinkActivity) 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 (org.sanfordhealth.patient.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.
5	Activity (org.sanfordhealth.patient.AppLinkActivity) 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.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.
7	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	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
11	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.
12	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.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewActivity.java 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/l

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	ogin/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/permissions/PermissionProminentDisclosure.java com/epic/patientengagement/core/security/SecurityPoints.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/WebService.java com/epic/patientengagement/core/webservice/processor/MyChartResponseProcessor.java com/epic/patientengagement/homepage/HomePageComponentAPI.java com/qualtrics/digital/EmbeddedFeedbackUtils.java com/qualtrics/digital/EmbeddedFeedbackUtilsJava.java com/qualtrics/digital/ExpressionDeserializer.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/SDKUtils.java com/qualtrics/digital/XMDUtils.java com/qualtrics/digital/utils/TranslationUtils.java epic/mychart/android/library/api/classes/WPAPIAuthentication.java epic/mychart/android/library/healthlinks/d.java expo/modules/adapters/react/NativeModulesProxy.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
				br/com/classapp/RNSensitiveInfo/RNSensitiveInfoModule.java com/epic/patientengagement/core/session/MyChartOrgToOrgJumpManager.java com/epic/patientengagement/core/ui/ProgressBar.java com/epic/patientengagement/core/ui/buttons/CoreButton.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/core/ui/buttons/FocusButtonUtils.java com/epic/patientengagement/core/ui/stickyheader/StickyHeaderAdapter.java com/epic/patientengagement/core/ui/tutorials/PETutorialFragment.java com/epic/patientengagement/core/utilities/PerformanceLogger.java com/epic/patientengagement/core/utilities/broadcast/BroadcastManager.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/epic/patientengagement/todo/progress/c.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/c.java com/learnium/RNDeviceInfo/resolver/a.java com/microsoft/codepush/react/f.java com/qualtrics/digital/ActionSet.java com/qualtrics/digital/DateExpression.java com/qualtrics/digital/DayExpression.java com/qualtrics/digital/DurationExpression.java com/qualtrics/digital/InterceptDefinition.java com/qualtrics/digital/Properties.java com/qualtrics/digital/Qualtrics.java com/qualtrics/digital/QualtricsLog.java com/qualtrics/digital/QualtricsPopOverFragment.java com/qualtrics/digital/QualtricsSurveyActivity.java com/qualtrics/digital/QualtricsSurveyExpression.java com/qualtrics/digital/ServiceInterceptor.java com/qualtrics/digital/TimeExpression.java com/qualtrics/digital/VariableExpression.java com/qualtrics/digital/ViewCountExpression.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/qualtrics/digital/WebViewInterface.java com/qualtrics/digital/resolvers/CustomPropertyResolver.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/qualtrics/digital/resolvers/DateTimeTypeResolvers.java com/qualtrics/digital/resolvers/QualtricsSurveyResolver.java com/qualtrics/digital/resolvers/SamplingResolver.java com/qualtrics/digital/resolvers/TimeSpentInAppResolver.java com/qualtrics/digital/resolvers/ViewCountResolver.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/reactnativecommunity/webview/d.java com/reactnativecommunity/webview/h.java com/rnmaps/maps/MapGradientPolyline.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/MapUrlTile.java com/rnmaps/maps/f.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/gesturehandler/react/i.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java epic/mychart/android/library/api/classes/WPAPIFirebaseMessagingService.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/appointments/c.java epic/mychart/android/library/campaigns/d.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java epic/mychart/android/library/customadapters/StickyHeaderSectionAdapter/c.java epic/mychart/android/library/general/AccessResult.java epic/mychart/android/library/general/DeepLinkManager.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/location/fragments/a.java epic/mychart/android/library/location/services/AppointmentArrivalService.java epic/mychart/android/library/pushnotifications/CustomFcmListenerService.java epic/mychart/android/library/trackmyhealth/a.java epic/mychart/android/library/utilities/e0.java epic/mychart/android/library/utilities/f0.java epic/mychart/android/library/utilities/j.java epic/mychart/android/library/utilities/k.java epic/mychart/android/library/utilities/p.java epic/mychart/android/library/utilities/r.java epic/mychart/android/library/utilities/z.java expo/modules/b.java expo/modules/constants/ConstantsService.java expo/modules/constants/c.java expo/modules/core/logging/d.java expo/modules/filesystem/f.java expo/modules/location/j.java expo/modules/location/records/GeocodeResponse.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/app/a.java io/invertase/firebase/common/g.java io/invertase/firebase/common/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/perf/i.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/nlopez/smartlocation/utils/c.java org/altbeacon/beacon/BeaconParser.java org/altbeacon/beacon/logging/ApiTrackingLogger.java org/altbeacon/beacon/logging/InfoAndroidLogger.java org/altbeacon/beacon/logging/VerboseAndroidLogger.java org/altbeacon/beacon/logging/WarningAndroidLogger.java org/altbeacon/beacon/service/ScanHelper.java org/altbeacon/beacon/service/ScanState.java org/altbeacon/beacon/utils/EddystoneTelemetryAccessor.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/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/qualtrics/digital/QualtricsSurveyFragment.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java
4	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 com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java epic/mychart/android/library/utilities/DeviceUtil.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
6	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 com/qualtrics/digital/SamplingUtil.java epic/mychart/android/library/utilities/r.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/reactnativecommunity/asyncstorage/f.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	expo/modules/adapters/react/permissions/e.java expo/modules/constants/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/a.java
10	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
11	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	epic/mychart/android/library/utilities/k.java
12	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

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	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/qualtrics/digital/QualtricsNotificationManager.java com/qualtrics/digital/QualtricsPopOverActivity.java com/qualtrics/digital/QualtricsSurveyFragment.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 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

RULE ID	BEHAVIOUR	LABEL	FILES
			expo/modules/adapters/react/permissions/e.java expo/modules/filesystem/f.java com/epic/patientengagement/pdfviewer/utilities/FileUtils.java
00013	Read file and put it into a stream	file	com/microsoft/codepush/react/e.java com/microsoft/codepush/react/i.java com/reactnativecommunity/asyncstorage/c.java com/rnmaps/maps/MapLocalTile.java com/rnmaps/maps/a.java com/rnmaps/maps/f.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 expo/modules/core/logging/f.java expo/modules/filesystem/f.java okio/o.java org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java org/altbeacon/beacon/service/MonitoringStatus.java org/altbeacon/beacon/service/ScanState.java
00091	Retrieve data from broadcast	collection	com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/qualtrics/digital/QualtricsNotificationManager.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 expo/modules/location/services/LocationTaskService.java
00147	Get the time of current location	collection location	expo/modules/location/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2$result$1.java com/microsoft/codepush/react/d.java
00089	Connect to a URL and receive input stream from the server	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/microsoft/codepush/react/d.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00030	Connect to the remote server through the given URL	network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.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
00108	Read the input stream from given URL	network command	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customobjects/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/epic/patientengagement/core/utilities/DeviceUtil.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/e.java com/microsoft/codepush/react/f.java com/microsoft/codepush/react/i.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java expo/modules/filesystem/f.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java org/altbeacon/beacon/service/ScanState.java
00024	Write file after Base64 decoding	reflection file	epic/mychart/android/library/messages/Attachment.java expo/modules/filesystem/f.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/qualtrics/digital/QualtricsNotificationManager.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java expo/modules/adapters/react/permissions/e.java
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/rnmaps/maps/MapMarker.java com/rnmaps/maps/d.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 expo/modules/adapters/react/permissions/e.java expo/modules/filesystem/f.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/k.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java expo/modules/filesystem/f.java
00202	Make a phone call	control	epic/mychart/android/library/utilities/k.java
00203	Put a phone number into an intent	control	epic/mychart/android/library/utilities/k.java
00012	Read data and put it into a buffer stream	file	com/microsoft/codepush/react/i.java epic/mychart/android/library/utilities/i.java expo/modules/filesystem/f.java
00153	Send binary data over HTTP	http	epic/mychart/android/library/utilities/g.java
00109	Connect to a URL and get the response code	network command	com/epic/patientengagement/core/webservice/WebServiceTask.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/codepush/react/f.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java
00121	Create a directory	file command	expo/modules/filesystem/f.java
00104	Check if the given path is directory	file	expo/modules/filesystem/f.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/rnmaps/maps/f.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://haiku-push-notifications.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://api-project-295670585778.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/295670585778/namespaces/firebase:fetch?key=AIzaSyDzE5zKF0C685w_yFjEhL6euUts9gnne60. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	7/44	android.permission.FOREGROUND_SERVICE, android.permission.CALL_PHONE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
codepush.appcenter.ms	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

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
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
survey.qualtrics.com	ok	**IP:** 23.202.57.104 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.datacontract.org	ok	**IP:** 207.46.232.160 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
www.mysanfordchart.org	ok	**IP:** 206.208.222.58 **Country:** United States of America **Region:** Minnesota **City:** Crookston **Latitude:** 47.774139 **Longitude:** -96.608124 **View:** Google Map
docs.swmansion.com	ok	**IP:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
future.mysanfordchart.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
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:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rex.webqa.epic.com	ok	No Geolocation information available.
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
mobilepreview.epic.com	ok	**IP:** 199.204.56.221 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **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
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
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
s-s.s	ok	No Geolocation information available.
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
s3.amazonaws.com	ok	**IP:** 52.217.142.16 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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
schemas.android.com	ok	No Geolocation information available.
altbeacon.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-project-295670585778.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
s.qualtrics.com	ok	**IP:** 23.202.57.104 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

EMAILS

EMAIL	FILE
example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"Branding_Google_Client_Secret" : "3_pgChSFtx4yM33e_FpsGMBF"
"Branding_MenuApplicationKey" : "SANFORD"
"CodePushDeploymentKey" : "9EKn-3Gw2rWQO3VtQgJA81G-paFwTPHYM0Few"
"com.google.firebase.crashlytics.mapping_file_id" : "1a1aa49a17734d2caa8ea323f216bbdc"
"firebase_database_url" : "https://api-project-295670585778.firebaseio.com"
"google_api_key" : "AIzaSyDzE5zKF0C685w_yFjEhL6euUts9gnne60"
"google_crash_reporting_api_key" : "AIzaSyDzE5zKF0C685w_yFjEhL6euUts9gnne60"
"wp_key_preferences_about" : "wp_preference_about"

POSSIBLE SECRETS
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_app_review_header" : "wp_preferences_app_review_header"
"wp_key_preferences_app_review_mode_switch" : "wp_key_preferences_app_review_mode_switch"
"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"
"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"

POSSIBLE SECRETS
"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"
"wp_two_factor_authentication_success_accessibility_announcement" : "Success!"
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
275801935599597058778490118403890480930569058563615685214287073019886892413098608651362607648837451077654397612305 75
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
49f946663a8deb7054212b8adda248c6
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148

POSSIBLE SECRETS
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
484395612939064517590525852527979142027629495260417479958440807170824046352 86
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
11579208921035624876269744694940757353008614341529031419553363130886709785395 1
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
c103703e120ae8cc73c9248622f3cd1e
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
11579208921035624876269744694940757353008614341529031419553363130886709785394 8
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Sanford

Score: 4.2540984 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.sanfordhealth.patient

Developer Details: Sanford Health, Sanford+Health, None, https://www.sanfordhealth.org, digitalmarketing@sanfordhealth.org,

Release Date: Apr 12, 2013 **Privacy Policy:** Privacy link

Description:

The Sanford Health App is a convenient way to manage your health information in one place. The app includes integrated access to My Sanford Chart, and a variety of solutions which are free to use and available 24/7. Easy-to-use features include: • Find a doctor and view patient satisfaction ratings • Find a location near you, and get directions • View acute/urgent care wait times • View your medical records • Access test results • Schedule appointments and receive reminders • Schedule a virtual visit • Securely message your doctor • Request prescription renewals or refills • Pay your bill *Access to your medical records requires you to have a My Sanford Chart account. You can create a My Sanford Chart account by selecting Sign-Up Online at: www.mysanfordchart.org

SCAN LOGS

Timestamp	Event	Error
2025-09-01 16:53:23	Generating Hashes	OK
2025-09-01 16:53:23	Extracting APK	OK

2025-09-01 16:53:23	Unzipping	OK
2025-09-01 16:53:25	Parsing APK with androguard	OK
2025-09-01 16:53:25	Extracting APK features using aapt/aapt2	OK
2025-09-01 16:53:25	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 16:53:28	Parsing AndroidManifest.xml	OK
2025-09-01 16:53:28	Extracting Manifest Data	OK
2025-09-01 16:53:28	Manifest Analysis Started	OK
2025-09-01 16:53:28	Reading Network Security config from wp_network_security_config.xml	OK
2025-09-01 16:53:28	Parsing Network Security config	OK
2025-09-01 16:53:28	Performing Static Analysis on: Sanford (org.sanfordhealth.patient)	OK
2025-09-01 16:53:30	Fetching Details from Play Store: org.sanfordhealth.patient	OK

2025-09-01 16:53:31	Checking for Malware Permissions	OK
2025-09-01 16:53:31	Fetching icon path	OK
2025-09-01 16:53:31	Library Binary Analysis Started	OK
2025-09-01 16:53:31	Reading Code Signing Certificate	OK
2025-09-01 16:53:31	Running APKiD 2.1.5	OK
2025-09-01 16:53:34	Detecting Trackers	OK
2025-09-01 16:53:38	Decompiling APK to Java with JADX	OK
2025-09-01 16:53:50	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 16:53:50	Decompiling classes6.dex with JADX	OK
2025-09-01 16:53:58	Decompiling classes2.dex with JADX	OK
2025-09-01 16:54:01	Decompiling classes4.dex with JADX	OK

2025-09-01 16:54:04	Decompiling classes.dex with JADX	OK
2025-09-01 16:54:12	Decompiling classes3.dex with JADX	OK
2025-09-01 16:54:15	Decompiling classes5.dex with JADX	OK
2025-09-01 16:54:23	Decompiling classes6.dex with JADX	OK
2025-09-01 16:54:31	Decompiling classes2.dex with JADX	OK
2025-09-01 16:54:34	Decompiling classes4.dex with JADX	OK
2025-09-01 16:54:36	Decompiling classes.dex with JADX	OK
2025-09-01 16:54:44	Decompiling classes3.dex with JADX	OK
2025-09-01 16:54:47	Decompiling classes5.dex with JADX	OK
2025-09-01 16:54:54	Converting DEX to Smali	OK
2025-09-01 16:54:54	Code Analysis Started on - java_source	OK

2025-09-01 16:54:57	Android SBOM Analysis Completed	OK
2025-09-01 16:55:03	Android SAST Completed	OK
2025-09-01 16:55:03	Android API Analysis Started	OK
2025-09-01 16:55:08	Android API Analysis Completed	OK
2025-09-01 16:55:09	Android Permission Mapping Started	OK
2025-09-01 16:55:13	Android Permission Mapping Completed	OK
2025-09-01 16:55:14	Android Behaviour Analysis Started	OK
2025-09-01 16:55:19	Android Behaviour Analysis Completed	OK
2025-09-01 16:55:19	Extracting Emails and URLs from Source Code	OK
2025-09-01 16:55:25	Email and URL Extraction Completed	OK
2025-09-01 16:55:25	Extracting String data from APK	OK

2025-09-01 16:55:25	Extracting String data from Code	OK
2025-09-01 16:55:25	Extracting String values and entropies from Code	OK
2025-09-01 16:55:30	Performing Malware check on extracted domains	OK
2025-09-01 16:55:32	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.