ANDROID STATIC ANALYSIS REPORT

myPennMedicine (10.9.3)

File Name:	org.secure.mypennmedicine.mypennmed_3126.apk
Package Name:	org.secure.mypennmedicine.mypennmed
Scan Date:	Sept. 1, 2025, 4:55 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	17	3	1	1

FILE INFORMATION

File Name: org.secure.mypennmedicine.mypennmed_3126.apk
Size: 39.3MB
MD5: 6aaea1259dd08afacc9859345a7bafca
SHA1: 93905ee6544dbd331826f2347a80fee840221d6c
SHA256: 78669b7e496e872ccfa092135a584c5266a8a65e2e15e5b467029553b08b7182

APP INFORMATION

App Name: myPennMedicine
Package Name: org.secure.mypennmedicine.mypennmed
Main Activity: epic.mychart.android.library.prelogin.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 10.9.3

Android Version Code: 3126

APP COMPONENTS

Activities: 92
Services: 15
Receivers: 7
Providers: 3
Exported Activities: 2
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, O=Penn Medicine
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-03-16 19:48:07+00:00
Valid To: 2048-03-08 19:48:07+00:00
Issuer: C=US, O=Penn Medicine
Serial Number: 0x118b632d
Hash Algorithm: sha256
md5: 9fa1d12082096e5c356a97dc5dde62f2
sha1: 8c061611027184fc123f5f283bdc6494e588b87b
sha256: 50668fbb3a57afac0e9de5be8945a534e73a59480652a2b7f15eef9b37b0e2eb
sha512: 271b188db8bff366e2f55936204164ae3c7b8f2327ac79278d4a44f30b89d05d164586dd6c733fa09c54ee2bbd96cc827e92e9c8fbe6a6a26ddcc9bca5825821
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 91434a42164eea2e1c79c16303fff23209266d55e354118795976ad9ad7bdf70
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.USE_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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
org.secure.mypennmedicine.mypennmed.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>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>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></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>
<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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

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

NETWORK SECURITY

HIGH: **2** | WARNING: **1** | INFO: **0** | SECURE: **0**

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

NO	SCOPE	SEVERITY	DESCRIPTION
3	*	high	Base config is configured to trust user installed certificates.

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: **7** | 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/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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	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.
5	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.
6	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
7	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.
8	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: **7** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/core/session/MyChartOrgToOrgJumpManager.java com/epic/patientengagement/core/ui/Progre

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	ssBar.java com/epic/patientengagement/core/ui/buttons/CoreButton.java com/epic/patientengagement/core/ui/buttons/CoreButtonUtils.java com/epic/patientengagement/core/ui/stickyheader/StickyHeaderAdapter.java com/epic/patientengagement/core/ui/tutorials/PETutorialFragment.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/b.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/f.java 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/c.java epic/mychart/android/library/location/fragments/e.java epic/mychart/android/library/location/services/AppointmentArrivalService.java epic/mychart/android/library/pushnotificatio

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ns/CustomFcmListenerService.java epic/mychart/android/library/trackmyhealth/a.java epic/mychart/android/library/utilities/c0.java epic/mychart/android/library/utilities/d2.java epic/mychart/android/library/utilities/e2.java epic/mychart/android/library/utilities/f0.java epic/mychart/android/library/utilities/m1.java epic/mychart/android/library/utilities/q0.java epic/mychart/android/library/utilities/y1.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
				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

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.]()	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/LoginHelper.java com/epic/patientengagement/authentication/login/utilities/LoginResultCode.java com/epic/patientengagement/authentication/login/utilities/OrganizationLoginHelper.java com/epic/patientengagement/authentication/login/utilities/SamlSessionManager.java com/epic/patientengagement/core/permissions/PermissionProminentDisclosure.java com/epic/patientengagement/homepage/HomePageComponentAPI.java com/epic/patientengagement/homepage/onboarding/a.java epic/mychart/android/library/api/classes/WPAPIAuthentication.java epic/mychart/android/library/healthlinks/e.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
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 epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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 epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/f0.java
5	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/f0.java
6	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
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/epic/patientengagement/core/utilities/EncryptionUtil.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/epic/patientengagement/core/utilities/EncryptionUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java epic/mychart/android/library/utilities/DeviceUtil.java
10	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/epic/patientengagement/homepage/itemfeed/webservice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/QuestionnaireSeries.java epic/mychart/android/library/utilities/m1.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 epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/campaigns/e.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/f.java epic/mychart/android/library/healthlinks/q0.java epic/mychart/android/library/insurance/e.java epic/mychart/android/library/letters/WebLettersActivity.java epic/mychart/android/library/personalize/e.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/f0.java epic/mychart/android/library/welcomewizard/WelcomeWizardWebViewFragmentManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/f0.java
00036	Get resource file from res/raw directory	reflection	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/f0.java
00091	Retrieve data from broadcast	collection	com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.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
00202	Make a phone call	control	epic/mychart/android/library/utilities/f0.java
00203	Put a phone number into an intent	control	epic/mychart/android/library/utilities/f0.java
00022	Open a file from given absolute path of the file	file	com/epic/patientengagement/core/utilities/DeviceUtil.java epic/mychart/android/library/customviews/VideoPlayerActivity.java epic/mychart/android/library/messages/Attachment.java org/altbeacon/beacon/service/ScanState.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/epic/patientengagement/pdfviewer/utilities/FileUtils.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/b0.java org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java org/altbeacon/beacon/service/MonitoringStatus.java org/altbeacon/beacon/service/ScanState.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 epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/s.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/s.java
00112	Get the date of the calendar event	collection calendar	epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/c.java epic/mychart/android/library/healthlinks/g0.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
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

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
00096	Connect to a URL and set request method	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/s.java
00153	Send binary data over HTTP	http	epic/mychart/android/library/utilities/s.java
00012	Read data and put it into a buffer stream	file	epic/mychart/android/library/utilities/b0.java
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.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/e.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java
00024	Write file after Base64 decoding	reflection file	epic/mychart/android/library/messages/Attachment.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://fifth-liberty-89719.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/706446232476/namespaces/firebase:fetch?key=AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	7/44	android.permission.CALL_PHONE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.pennmedicine.org	ok	**IP:** 45.60.75.182 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **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
schemas.datacontract.org	ok	**IP:** 207.46.197.115 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
haiku-push-notifications.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
secure.mypennmedicine.org	ok	**IP:** 45.60.75.182 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **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
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

DOMAIN	STATUS	GEOLOCATION
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
s3.amazonaws.com	ok	**IP:** 52.217.197.0 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 172.217.21.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
fifth-liberty-89719.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
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
example@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://fifth-liberty-89719.firebaseio.com"
"google_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"google_crash_reporting_api_key" : "AIzaSyBv776FvkVLGKyvr4AR_IFvkThhUx18A2s"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"

POSSIBLE SECRETS
"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"
"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"

POSSIBLE SECRETS
"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!"

PLAYSTORE INFORMATION

Title: myPennMedicine

Score: 4.7619047 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.secure.mypennmedicine.mypennmed

Developer Details: Penn Medicine, Penn+Medicine, None, https://secure.mypennmedicine.org, mypennmedicineapp@pennmedicine.upenn.edu,

Release Date: Sep 16, 2019 **Privacy Policy:** Privacy link

Description:

The myPennMedicine app offers Penn Medicine patients easy, secure access to your personal medical records. An on-the-go connection to the information you need most: test results, referrals, prescribed medications and refill requests, appointment scheduling and more including syncing your Apple Health compatible tracking device to myPennMedicine. You can also communicate with your care team through secure messaging in the myPennMedicine app. Learn more at myPennMedicine.org. Penn Medicine hospitals are ranked among the top hospitals in the country by U.S. News & World Report and recognized as among the Philadelphia region’s best health care. Learn more at PennMedicine.org.

SCAN LOGS

Timestamp	Event	Error

2025-09-01 16:55:38	Generating Hashes	OK
2025-09-01 16:55:38	Extracting APK	OK
2025-09-01 16:55:38	Unzipping	OK
2025-09-01 16:55:38	Parsing APK with androguard	OK
2025-09-01 16:55:39	Extracting APK features using aapt/aapt2	OK
2025-09-01 16:55:39	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 16:55:42	Parsing AndroidManifest.xml	OK
2025-09-01 16:55:42	Extracting Manifest Data	OK
2025-09-01 16:55:42	Manifest Analysis Started	OK
2025-09-01 16:55:42	Reading Network Security config from wp_network_security_config.xml	OK
2025-09-01 16:55:42	Parsing Network Security config	OK

2025-09-01 16:55:42	Performing Static Analysis on: myPennMedicine (org.secure.mypennmedicine.mypennmed)	OK
2025-09-01 16:55:43	Fetching Details from Play Store: org.secure.mypennmedicine.mypennmed	OK
2025-09-01 16:55:45	Checking for Malware Permissions	OK
2025-09-01 16:55:45	Fetching icon path	OK
2025-09-01 16:55:45	Library Binary Analysis Started	OK
2025-09-01 16:55:45	Reading Code Signing Certificate	OK
2025-09-01 16:55:45	Running APKiD 2.1.5	OK
2025-09-01 16:55:47	Detecting Trackers	OK
2025-09-01 16:55:51	Decompiling APK to Java with JADX	OK
2025-09-01 16:56:05	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 16:56:05	Decompiling classes2.dex with JADX	OK

2025-09-01 16:56:09	Decompiling classes4.dex with JADX	OK
2025-09-01 16:56:11	Decompiling classes.dex with JADX	OK
2025-09-01 16:56:19	Decompiling with JADX failed for classes.dex	OK
2025-09-01 16:56:19	Decompiling classes3.dex with JADX	OK
2025-09-01 16:56:24	Decompiling classes5.dex with JADX	OK
2025-09-01 16:56:30	Decompiling classes2.dex with JADX	OK
2025-09-01 16:56:34	Decompiling classes4.dex with JADX	OK
2025-09-01 16:56:36	Decompiling classes.dex with JADX	OK
2025-09-01 16:56:44	Decompiling classes3.dex with JADX	OK
2025-09-01 16:56:49	Decompiling classes5.dex with JADX	OK
2025-09-01 16:56:55	Some DEX files failed to decompile	OK

2025-09-01 16:56:55	Converting DEX to Smali	OK
2025-09-01 16:56:55	Code Analysis Started on - java_source	OK
2025-09-01 16:56:58	Android SBOM Analysis Completed	OK
2025-09-01 16:57:03	Android SAST Completed	OK
2025-09-01 16:57:03	Android API Analysis Started	OK
2025-09-01 16:57:07	Android API Analysis Completed	OK
2025-09-01 16:57:08	Android Permission Mapping Started	OK
2025-09-01 16:57:12	Android Permission Mapping Completed	OK
2025-09-01 16:57:12	Android Behaviour Analysis Started	OK
2025-09-01 16:57:18	Android Behaviour Analysis Completed	OK
2025-09-01 16:57:18	Extracting Emails and URLs from Source Code	OK

2025-09-01 16:57:22	Email and URL Extraction Completed	OK
2025-09-01 16:57:22	Extracting String data from APK	OK
2025-09-01 16:57:23	Extracting String data from Code	OK
2025-09-01 16:57:23	Extracting String values and entropies from Code	OK
2025-09-01 16:57:28	Performing Malware check on extracted domains	OK
2025-09-01 16:57:30	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.