MOBSF

ANDROID STATIC ANALYSIS REPORT

FollowMyHealth (24.4)

File Name:	com.jardogs.fmhmobile_1548.apk
Package Name:	com.jardogs.fmhmobile
Scan Date:	Aug. 30, 2025, 10:27 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	13	4	2	1

FILE INFORMATION

File Name: com.jardogs.fmhmobile_1548.apk
Size: 48.31MB
MD5: fc134926aca026c122bbaa29265b1e5d
SHA1: b9c028ef0379efd40b358c410064ddc413f7decb
SHA256: c7000dcd7cdff787fbe56f7ac94c52207f65b9e8fc2a6e2f1d3960b76b0d532c

APP INFORMATION

App Name: FollowMyHealth
Package Name: com.jardogs.fmhmobile
Main Activity: com.jardogs.fmhmobile.library.activities.EntryPointActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 24.4

Android Version Code: 1548

APP COMPONENTS

Activities: 60
Services: 11
Receivers: 4
Providers: 3
Exported Activities: 1
Exported Services: 1
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: O=Jardogs
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-08-06 22:51:26+00:00
Valid To: 2037-07-31 22:51:26+00:00
Issuer: O=Jardogs
Serial Number: 0x50204a6e
Hash Algorithm: sha1
md5: 7cefc15f31e7911b0688935eebd468fb
sha1: eb637c892e0a0bfe1918303d7cea2e8b19779984
sha256: f1d3d499d16ba006daed3b0356b97d3b686aef871f7fc1826e767155d648a62d
sha512: 4c6428f03c29d2a619d1ac513ec2ee88c9a2616ed824daaa9fe984fcf70edf5d40d41b9e5b42087207b3f13522ffcec5e9399ba64b9edf4d91eeba3531827fca
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 903f60e3d9ebbcbad3df99223b44000af8cfcd6169dfc23489f5ae1dd79b1316
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
fc134926aca026c122bbaa29265b1e5d.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

FILE	DETAILS
classes.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.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.TAGS check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<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>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.jardogs.fmhmobile.library.activities.LoginSelectorActivity	Schemes: fmh://,
com.jardogs.fmhmobile.library.activities.EntryPointActivity	Schemes: fmhvv://, fmhsvv://, fmhapp://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	support.followmyhealth.com assistly-production.s3.amazonaws.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	Activity (com.jardogs.fmhmobile.library.activities.LoginSelectorActivity) 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.
3	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.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				butterknife/ButterKnife.java com/fondesa/kpermissions/request/runtime/DefaultFragmentRuntimePermissionHandler.java com/highsoft/highcharts/core/HIChartView.java com/highsoft/highcharts/core/e.java com/hunter/library/debug/HunterLoggerHandler.java com/hunter/library/debug/ParameterPrinter.java com/hunter/library/debug/ResultPrinter.java com/hunter/library/debug/TimingLogger.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/LocalLog.java com/jardogs/fmhmobile/library/activities/EntryPointActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/jardogs/fmhmobile/library/activities/support/VidyoDetails.java com/jardogs/fmhmobile/library/utility/Util.java com/jardogs/fmhmobile/library/views/base/RecyclerViewSingleSelectionPresenter.java com/jardogs/fmhmobile/library/views/evisit/AttachmentsManager.java com/jardogs/fmhmobile/library/views/evisit/request/EVisitOrganizationAndProviderRequest.java com/jardogs/fmhmobile/library/views/healthrecord/uploading/AddResultsActivity.java com/jardogs/fmhmobile/library/views/home/HomeViewModel$createSsoUrl$1.java com/jardogs/fmhmobile/library/views/home/type/ResourceCenterItemWithDisplayMoreFlag.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModel$registerDeviceForPush$1.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModel$setUpData$1.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModel$unregisterDeviceForPush$1.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModel$updateCommunicationPreferences$1.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModelFactory.java com/jardogs/fmhmobile/library/views/videovisit/newpatient/ondemand/NewPatientODVVPresenter$connectVidyo$1.java com/jardogs/fmhmobile/library/views/videovisit/newpatient/ondemand/NewPatientODVVWaitingRoomPresenter.java com/jardogs/fmhmobile/library/views/videovisit/repo/UnsecuredVisitRepo.java com/jardogs/fmhmobile/library/views/vidyo/NewPatientODVidyoSessionView.java com/jardogs/fmhmobile/library/views/vidyo/VidyoSessionView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/loopeer/itemtouchhelperextension/ItemTouchHelperExtension.java com/vidyo/lmi/BatteryManager.java com/vidyo/lmi/LocationManager.java com/vidyo/lmi/ScreenManager.java com/vidyo/lmi/ui/Window.java icepick/Icepick.java net/zetetic/database/DatabaseUtils.java net/zetetic/database/DefaultDatabaseErrorHandler.java net/zetetic/database/sqlcipher/CloseGuard.java net/zetetic/database/sqlcipher/SQLiteConnection.java net/zetetic/database/sqlcipher/SQLiteConnectionPool.java net/zetetic/database/sqlcipher/SQLiteCursor.java net/zetetic/database/sqlcipher/SQLiteDatabase.java net/zetetic/database/sqlcipher/SQLiteDebug.java net/zetetic/database/sqlcipher/SQLiteOpenHelper.java net/zetetic/database/sqlcipher/SQLiteQuery.java net/zetetic/database/sqlcipher/SQLiteQueryBuilder.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/slf4j/helpers/Util.java retrofit/Platform.java retrofit/android/AndroidLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java net/zetetic/database/DatabaseUtils.java net/zetetic/database/sqlcipher/SQLiteDatabase.java
3	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/jardogs/fmhmobile/library/activities/base/BaseActivity.java com/jardogs/fmhmobile/library/dialogs/FilePickerDialog.java com/jardogs/fmhmobile/library/views/documents/AddScannedDocumentActivity.java com/jardogs/fmhmobile/library/views/documents/request/DownloadClinicalFileRequest.java com/jardogs/fmhmobile/library/views/healthrecord/export/ExportDocumentSendFragment.java com/jardogs/fmhmobile/library/views/home/HomeFragmentList.java
4	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/jardogs/fmhmobile/library/db/FMHDBPinHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/jardogs/fmhmobile/library/dialogs/FilePickerDialog.java com/jardogs/fmhmobile/library/views/documents/AddScannedDocumentActivity.java com/jardogs/fmhmobile/library/views/home/HomeFragmentList.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/jardogs/fmhmobile/library/activities/support/VidyoDetails.java com/jardogs/fmhmobile/library/db/fmh/MigratingOrmLiteSqliteOpenHelper.java com/jardogs/fmhmobile/library/service/FMHNotificationListenerService.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/DecoratedDatePickerPresenter.java com/jardogs/fmhmobile/library/views/journal/HealthJournalPagerActivity.java com/jardogs/fmhmobile/library/views/login/UsernameRecoveryWebView.java com/jardogs/fmhmobile/library/views/settings/ChangePasswordActivity.java com/jardogs/fmhmobile/library/views/settings/ChangeUsernameActivity.java com/jardogs/fmhmobile/library/views/settings/ChangeUsernameActivityKt.java com/jardogs/fmhmobile/library/views/settings/ChangeUsernamePasswordViewModel.java com/jardogs/fmhmobile/library/views/settings/CommunicationPreferencesViewModelKt.java com/jardogs/fmhmobile/library/views/settings/PasswordDTO.java com/jardogs/fmhmobile/library/views/settings/TwoFactorDTO.java com/jardogs/fmhmobile/library/views/support/SupportRequestViewModelKt.java io/jsonwebtoken/JwsHeader.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/highsoft/highcharts/core/HIChartView.java com/jardogs/fmhmobile/library/views/billing/BillPayWebViewActivity.java com/jardogs/fmhmobile/library/views/forms/FormViewPresenter.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/jardogs/fmhmobile/library/views/settings/TwoFactorAuthActivity.java
9	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/jardogs/fmhmobile/library/db/pin/Pin.java com/jardogs/fmhmobile/library/fingerprint/AuthenticationMediator.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/jardogs/fmhmobile/library/services/PatientApiBuilder.java com/jardogs/fmhmobile/library/services/servicecalls/FMHImageService.java
11	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/jardogs/fmhmobile/library/activities/EntryPointActivity.java
12	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/jardogs/fmhmobile/library/activities/LoginActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/jardogs/fmhmobile/library/activities/LoginActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/jardogs/fmhmobile/library/activities/LoginActivity.java com/jardogs/fmhmobile/library/activities/VidyoActivity.java com/jardogs/fmhmobile/library/views/scheduledvideovisit/ScheduledVideoVisitPresenter.java com/jardogs/fmhmobile/library/views/videovisit/VideoVisitActivity.java
00075	Get location of the device	collection location	com/location/general/LocationService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/highsoft/highcharts/core/g.java com/jardogs/fmhmobile/library/activities/LoginActivity.java com/jardogs/fmhmobile/library/activities/LoginSelectorActivity.java com/jardogs/fmhmobile/library/activities/SSOActivity.java com/jardogs/fmhmobile/library/custom/AppReviewView.java com/jardogs/fmhmobile/library/dialogs/UpdateAppDialog.java com/jardogs/fmhmobile/library/utility/FMHExtensionsKt.java com/jardogs/fmhmobile/library/views/appcenter/HealthToolsListPresenter.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findprovider/ProviderDetailsPresenter$establishView$1.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/FindATimeMasterPresenter$viewEstablished$9.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/IndirectShimView$populateShim$7.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/LocationShimView.java com/jardogs/fmhmobile/library/views/billing/BillingGroupViewFragment.java com/jardogs/fmhmobile/library/views/email/EmailSingleView.java com/jardogs/fmhmobile/library/views/home/ActionCenterViewHolder.java com/jardogs/fmhmobile/library/views/home/ResourceCenterAdapter.java com/jardogs/fmhmobile/library/views/login/UsernameRecoveryWebView.java com/jardogs/fmhmobile/library/views/myhealth/RecordsViewPresenter.java com/jardogs/fmhmobile/library/views/prescriptioncard/PrescriptionCardHomeFragment.java com/jardogs/fmhmobile/library/views/rxrenewal/PharmacySearchPresenter$onEvent$7.java com/jardogs/fmhmobile/library/views/rxrenewal/PreferredPharmacyView.java com/jardogs/fmhmobile/library/views/rxrenewal/RxRenewalPresenter.java com/jardogs/fmhmobile/library/views/settings/PharmacySettingsActivity.java com/jardogs/fmhmobile/library/views/support/CommonSupportTopicsFragment.java com/jardogs/fmhmobile/library/views/support/SupportFragment.java com/jardogs/fmhmobile/library/views/support/SupportOrgListFragment$refreshViews$3.java com/jardogs/fmhmobile/library/views/util/BaseFragmentWebView.java com/jardogs/fmhmobile/library/views/util/Directions.java com/jardogs/fmhmobile/library/views/videovisit/VideoSessionSummaryView.java com/jardogs/fmhmobile/library/views/videovisit/newpatient/ondemand/NewPatientODVVPresenter.java com/jardogs/fmhmobile/library/views/videovisit/newpatient/shared/NewPatientPermissionPr

RULE ID	BEHAVIOUR	LABEL	FILES
			esenter.java
			com/jardogs/fmhmobile/library/views/appointments/scheduling2/findprovider/ProviderDetailsPresenter$establishView$1.java
00202	Make a phone call	control	com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/FindATimeMasterPresenter$viewEstablished$9.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/IndirectShimView$populateShim$7.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/LocationShimView.java com/jardogs/fmhmobile/library/views/rxrenewal/PharmacySearchPresenter$onEvent$7.java com/jardogs/fmhmobile/library/views/rxrenewal/PreferredPharmacyView.java com/jardogs/fmhmobile/library/views/rxrenewal/RxRenewalPresenter.java com/jardogs/fmhmobile/library/views/settings/PharmacySettingsActivity.java com/jardogs/fmhmobile/library/views/support/SupportOrgListFragment$refreshViews$3.java com/jardogs/fmhmobile/library/views/videovisit/VideoSessionSummaryView.java
00203	Put a phone number into an intent	control	com/jardogs/fmhmobile/library/views/appointments/scheduling2/findprovider/ProviderDetailsPresenter$establishView$1.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/FindATimeMasterPresenter$viewEstablished$9.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/IndirectShimView$populateShim$7.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/LocationShimView.java com/jardogs/fmhmobile/library/views/rxrenewal/PharmacySearchPresenter$onEvent$7.java com/jardogs/fmhmobile/library/views/rxrenewal/PreferredPharmacyView.java com/jardogs/fmhmobile/library/views/rxrenewal/RxRenewalPresenter.java com/jardogs/fmhmobile/library/views/settings/PharmacySettingsActivity.java com/jardogs/fmhmobile/library/views/support/SupportOrgListFragment$refreshViews$3.java com/jardogs/fmhmobile/library/views/videovisit/VideoSessionSummaryView.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/jardogs/fmhmobile/library/custom/AppReviewView.java com/jardogs/fmhmobile/library/dialogs/UpdateAppDialog.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findprovider/ProviderDetailsPresenter$establishView$1.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/FindATimeMasterPresenter$viewEstablished$9.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/IndirectShimView$populateShim$7.java com/jardogs/fmhmobile/library/views/appointments/scheduling2/findtime/LocationShimView.java com/jardogs/fmhmobile/library/views/rxrenewal/PharmacySearchPresenter$onEvent$7.java com/jardogs/fmhmobile/library/views/rxrenewal/PreferredPharmacyView.java com/jardogs/fmhmobile/library/views/rxrenewal/RxRenewalPresenter.java com/jardogs/fmhmobile/library/views/settings/PharmacySettingsActivity.java com/jardogs/fmhmobile/library/views/support/CommonSupportTopicsFragment.java com/jardogs/fmhmobile/library/views/support/SupportFragment.java com/jardogs/fmhmobile/library/views/support/SupportOrgListFragment$refreshViews$3.java com/jardogs/fmhmobile/library/views/videovisit/VideoSessionSummaryView.java com/jardogs/fmhmobile/library/views/videovisit/newpatient/shared/NewPatientPermissionPresenter.java
00013	Read file and put it into a stream	file	com/j256/ormlite/android/apptools/OrmLiteSqliteOpenHelper.java com/jardogs/fmhmobile/library/db/fmh/OrmLiteSqliteOpenHelper.java okio/Okio__JvmOkioKt.java retrofit/mime/TypedFile.java
00022	Open a file from given absolute path of the file	file	com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/jakewharton/picasso/OkHttp3Downloader.java net/zetetic/database/sqlcipher/SQLiteDatabase.java retrofit/mime/TypedFile.java
00089	Connect to a URL and receive input stream from the server	command network	com/jardogs/fmhmobile/library/services/servicecalls/FMHImageService.java com/jardogs/fmhmobile/library/utility/IOUtils.java retrofit/client/UrlConnectionClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/jardogs/fmhmobile/library/utility/IOUtils.java
00108	Read the input stream from given URL	network command	com/jardogs/fmhmobile/library/utility/IOUtils.java
00002	Open the camera and take picture	camera	com/jardogs/fmhmobile/library/activities/CameraActivity.java
00183	Get current camera parameters and change the setting.	camera	com/jardogs/fmhmobile/library/activities/CameraActivity.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/jardogs/fmhmobile/library/activities/CameraActivity.java
00208	Capture the contents of the device screen	collection screen	com/jardogs/fmhmobile/library/views/videovisit/screenshare/DeviceScreenShareSource.java
00112	Get the date of the calendar event	collection calendar	com/jardogs/fmhmobile/library/views/appointments/models/AppointmentSummary.java
00036	Get resource file from res/raw directory	reflection	com/jardogs/fmhmobile/library/custom/AppReviewView.java com/jardogs/fmhmobile/library/dialogs/UpdateAppDialog.java com/jardogs/fmhmobile/library/utility/FMHExtensionsKt.java com/jardogs/fmhmobile/library/views/billing/BillingGroupViewFragment.java com/jardogs/fmhmobile/library/views/home/ActionCenterViewHolder.java
00096	Connect to a URL and set request method	command network	retrofit/client/UrlConnectionClient.java
00109	Connect to a URL and get the response code	network command	retrofit/client/UrlConnectionClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	com/highsoft/highcharts/core/d.java
00102	Set the phone speaker on	command	com/vidyo/lmi/audio/AudioCentral.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://trim-webbing-95818.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/522028682465/namespaces/firebase:fetch?key=AIzaSyBfCjR5oby_anE60i8inEu5D32jaZQ3h5k. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
followmyhealth--fmhdev.my.salesforce.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
pay.google.com	ok	**IP:** 142.251.2.92 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.followmyhealth.com	ok	**IP:** 20.241.26.162 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
trim-webbing-95818.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.google.com	ok	**IP:** 142.250.72.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
tools.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 142.250.68.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.cdc.gov	ok	**IP:** 23.52.208.211 **Country:** Argentina **Region:** Ciudad Autonoma de Buenos Aires **City:** Buenos Aires **Latitude:** -34.613152 **Longitude:** -58.377232 **View:** Google Map
www.followmyhealth.com	ok	**IP:** 52.240.136.216 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
aka.ms	ok	**IP:** 184.27.213.254 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
www.followmyhealth.ca	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.followmyhealth.co.uk	ok	No Geolocation information available.
fmhqareleasepublic.blob.core.windows.net	ok	**IP:** 20.150.67.68 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
followmyhealth.glicrx.com	ok	**IP:** 52.70.48.249 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
followmyhealth.my.salesforce.com	ok	**IP:** 155.226.145.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
maps.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
www.followmyhealth	ok	No Geolocation information available.
prod-premium-wellness-wordpress.azurewebsites.net	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
fmhintegration@allscripts.com	com/jardogs/fmhmobile/library/views/support/SupportRequestViewModel$requestAuthString$1.java
fmhintegration@allscripts.com	com/jardogs/fmhmobile/library/views/support/SupportRequestViewModelKt.java
someone@domain.com example@email.com	Android String Resource

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "dda5f7689f234672932c0f5a7bdce226"
"credentials" : "Credentials"
"firebase_database_url" : "https://trim-webbing-95818.firebaseio.com"
"google_api_key" : "AIzaSyBfCjR5oby_anE60i8inEu5D32jaZQ3h5k"
"google_crash_reporting_api_key" : "AIzaSyBfCjR5oby_anE60i8inEu5D32jaZQ3h5k"
"login_password" : "Password"
"login_username" : "Username"
23456789abcdefghjkmnpqrstvwxyz
h9Ub79BgHoBmthzGvuEa6gRZ9PYF6vumyL7V0G20I5x3bUDKjNdgN3jrtPlX634R45m
YGGJglzircsrTSMTI1hpKT8FxTYRsnTb7CsroiAEI2m6AMxNTvFDxmc
eyJ0eXAiOiAiSldUIiwgImFsZyI6ICJSUzI1NiIsICJraWQiOiAiNTkyNmRiMDg3NmNkMDdmYWI2NTU5YzFjMDk0N2Q1MjRkM2ZmYWIyZiJ9
470fa2b4ae81cd56ecbcda9735803434cec591fa
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
3BB3229D-32DD-45DF-9687-F9C9A1E9770B

POSSIBLE SECRETS
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
3MVG9S6qnsIUe5wDH7s1r7xavm5VZA18fYx7
19604A2A-D496-4156-8C9D-F74CCB31CAEA
0qCADEe5auXkjYwg6eqCntaYNTFRvSnlU4Q9FbZUWwjJuiNB1SDwgpSzGwhMaRjWPgwyW5J4nmLQB1ZCY3Ss1hYmXMq0
6F995C352991FC632E851AA29DC162B7E21ECE106E3114662E2E63CB29575131
PDNEnstWLjMgoitNMUgotQs3nh5FB8xWrQCRL6JgozGznigicz93ueJgsBxtXeh7QbjvHtX
eyJpc3MiOiAiZm1oLW1vYmlsZUBhcGktNjM1MDg1NTY0NjAzMjM1MTA5Mi0yMjczOTIuaWFtLmdzZXJ2aWNlYWNjb3VudC5jb20iLCAiYXVkIjogImdvb2dsZSIsICJpYXQiOiAxNzM0MTI0OTkyLCAidHlwIjogInNhdmV0b3dhbGxldCIsICJwYXlsb2FkIjogeyJnZW5lcmljT2JqZWN0cyI6IFt7ImlkIjogIjMzODgwMDAwMDAwMjIzNjY0MzMuUHJlc2NyaXB0aW9uUGx1c19vYmplY3RfUFJPRCIsICJjbGFzc0lkIjogIjMzODgwMDAwMDAwMjIzNjY0MzMuUHJlc2NyaXB0aW9uUGx1c19jbGFzc19QUk9EIn1dfX0
7B298315-A00C-4743-BF98-7B012E14CD21
D7632B0E-F302-49AB-B10C-765B1E2CED68
nPCwemr5GIfFdU8RLV5jWHXh9Mo
D7B63046-5838-4C04-8070-D45F942F76B2
4D55A644-EB9B-4594-B625-105BE97418D1
50B340A23913ED368FEC57AC0F1FD8F57F8AD9DFA796AB56CD0BFC8F61D9DE44

PLAYSTORE INFORMATION

Title: FollowMyHealth®

Score: 4.747847 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.jardogs.fmhmobile

Developer Details: Veradigm LLC, Veradigm+LLC, None, https://support.followmyhealth.com/, fmhmobilefeedback@veradigm.com,

Release Date: Aug 6, 2012 **Privacy Policy:** Privacy link

Description:

Access and manage your health information on-the-go with the mobile version of your Universal Health Record powered by FollowMyHealth®. View test and lab results, request prescription renewals, communicate securely with your physicians, schedule appointments, and more – for you and your family with 24/7 online access!

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:27:42	Generating Hashes	OK
2025-08-30 22:27:42	Extracting APK	OK
2025-08-30 22:27:42	Unzipping	OK
2025-08-30 22:27:43	Parsing APK with androguard	OK
2025-08-30 22:27:44	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:27:44	Getting Hardcoded Certificates/Keystores	OK

2025-08-30 22:27:47	Parsing AndroidManifest.xml	OK
2025-08-30 22:27:47	Extracting Manifest Data	OK
2025-08-30 22:27:47	Manifest Analysis Started	OK
2025-08-30 22:27:47	Reading Network Security config from network_security_config.xml	OK
2025-08-30 22:27:47	Parsing Network Security config	OK
2025-08-30 22:27:47	Performing Static Analysis on: FollowMyHealth (com.jardogs.fmhmobile)	OK
2025-08-30 22:27:48	Fetching Details from Play Store: com.jardogs.fmhmobile	OK
2025-08-30 22:27:48	Checking for Malware Permissions	OK
2025-08-30 22:27:48	Fetching icon path	OK
2025-08-30 22:27:48	Library Binary Analysis Started	OK

2025-08-30 22:27:48	Reading Code Signing Certificate	OK
2025-08-30 22:27:49	Running APKiD 2.1.5	OK
2025-08-30 22:27:51	Detecting Trackers	OK
2025-08-30 22:27:55	Decompiling APK to Java with JADX	OK
2025-08-30 22:31:45	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-30 22:31:45	Decompiling classes2.dex with JADX	OK
2025-08-30 22:31:55	Decompiling classes.dex with JADX	OK
2025-08-30 22:32:07	Decompiling classes3.dex with JADX	OK
2025-08-30 22:32:16	Decompiling classes2.dex with JADX	OK
2025-08-30 22:32:26	Decompiling classes.dex with JADX	OK

2025-08-30 22:32:37	Decompiling classes3.dex with JADX	OK
2025-08-30 22:32:45	Converting DEX to Smali	OK
2025-08-30 22:32:45	Code Analysis Started on - java_source	OK
2025-08-30 22:32:49	Android SBOM Analysis Completed	OK
2025-08-30 22:32:59	Android SAST Completed	OK
2025-08-30 22:32:59	Android API Analysis Started	OK
2025-08-30 22:33:07	Android API Analysis Completed	OK
2025-08-30 22:33:07	Android Permission Mapping Started	OK
2025-08-30 22:33:14	Android Permission Mapping Completed	OK
2025-08-30 22:33:15	Android Behaviour Analysis Started	OK

2025-08-30 22:33:24	Android Behaviour Analysis Completed	OK
2025-08-30 22:33:24	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:33:29	Email and URL Extraction Completed	OK
2025-08-30 22:33:29	Extracting String data from APK	OK
2025-08-30 22:33:29	Extracting String data from Code	OK
2025-08-30 22:33:29	Extracting String values and entropies from Code	OK
2025-08-30 22:33:33	Performing Malware check on extracted domains	OK
2025-08-30 22:33:39	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.