MOBSF

ANDROID STATIC ANALYSIS REPORT

My IU Health (102.0.29)

File Name:	org.iuhealth.healthelife.play_39.apk
Package Name:	org.iuhealth.healthelife.play
Scan Date:	Sept. 1, 2025, 3:20 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	13	3	3	1

FILE INFORMATION

File Name: org.iuhealth.healthelife.play_39.apk
Size: 19.45MB
MD5: c2bb161de3371c14a405080c04090851
SHA1: 6ec7576b9268b4b8eb1157fb9e50d8ae16dad034
SHA256: 454a5b7f3746e4a6be00964ec9eb93291e4ec69b63f8cbf12b606ea1a36a2918

APP INFORMATION

App Name: My IU Health
Package Name: org.iuhealth.healthelife.play
Main Activity: com.cerner.healthelife_android.presenter.MainWebViewActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 102.0.29

Android Version Code: 39

APP COMPONENTS

Activities: 14
Services: 11
Receivers: 12
Providers: 4
Exported Activities: 0
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-07-06 15:26:43+00:00
Valid To: 2052-07-06 15:26:43+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x1618303b6bbbc8884723d29738695d58f763429
Hash Algorithm: sha256
md5: 6c0325cde021199a1f0e96e1222a8e62
sha1: 8284a54bbbff261eed919928ebb5e9b1dad00827
sha256: 1b487631f49ee882251017a0df0e53b1fe645dae204de81dd6d3bbc50c2d3656
sha512: 5c555db0f10d4d5c7818b6cc95830792e1b42c242c836000cedc5097306d14a9e944699b1cc36893da6ed773e1cc8d2354e1d02456dbdef2fba6d7b80926021c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a42f786a20431ac0a9bb70a8292d7984c3b00ac306ecd193cd4cfa07527998e7
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.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.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.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_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
org.iuhealth.healthelife.play.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS / DETAILS

FINDINGS	DETAILS
yara_issue	yara issue - dex file recognized by apkid but not yara module
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check SIM operator check
Compiler	unknown (please file detection issue!)

<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.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.cerner.healthelife_android.presenter.MainWebViewActivity	Schemes: org.iuhealth.healthelife.play://, https://, Hosts: tenants, app, iuhealth.consumermobile.us-1.healtheintent.com, Paths: /url, /auth, /store/android/org.iuhealth.healthelife.play, /oauth/redirect/org.iuhealth.healthelife.play,

NETWORK SECURITY

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

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

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

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	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.
5	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
6	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: **6** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				butterknife/ButterKnife.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/mediastore/c.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/prefill/a.java com/bumptech/glide/load/engine/r.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/Ha

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rdwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/a.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/j.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SimpleAssetResolver

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	.java com/caverock/androidsvg/b.java com/caverock/androidsvg/e.java com/caverock/androidsvg/f.java com/cerner/healthelife_android/libraries/hlbiometriccryptography/utils/BiometricCryptoOperator.java com/cerner/healthelife_android/libraries/hlcommonslib/sharedPreferences/HLSharePreference.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseWebViewActivity.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/util/HLWebViewUtil.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/webclients/HLBaseWebViewClient.java com/cerner/healthelife_android/presenter/MainWebViewActivity.java com/newrelic/agent/android/AndroidAgentImpl.java com/newrelic/agent/android/NewRelic.java com/newrelic/agent/android/SavedState.java com/newrelic/agent/android/agentdata/AgentDataController.java com/newrelic/agent/android/analytics/AnalyticsControllerImpl.java com/newrelic/agent/android/analytics/EventManagerImpl.java com/newrelic/agent/android/crash/UncaughtExceptionHandler.java com/newrelic/agent/android/harvest/Harvest.java com/newrelic/agent/android/hybrid/data/DataController.java com/newrelic/agent/android/instrumentation/io/CountingInputStream.java com/newrelic/agent/android/logging/AndroidAgentLog.java com/newrelic/agent/android/logging/ConsoleA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/newrelic/agent/android/logging/ConsoleAgentLog.java com/newrelic/agent/android/rum/AppApplicationLifeCycle.java com/newrelic/agent/android/sample/Sampler.java com/newrelic/agent/android/stores/SharedPrefsAnalyticsAttributeStore.java com/newrelic/agent/android/tracing/ActivityTrace.java com/newrelic/agent/android/tracing/TraceMachine.java com/samsung/android/sdk/healthdata/HealthDataObserver.java com/samsung/android/sdk/healthdata/HealthDataStore.java com/samsung/android/sdk/healthdata/HealthPermissionManager.java com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java com/samsung/android/sdk/internal/healthdata/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthdata/StreamUtil.java com/scottyab/aescrypt/AESCrypt.java com/validic/common/BitmapUtil.java com/validic/mobile/SessionData.java com/validic/mobile/SessionImpl.java com/validic/mobile/SingleRecordRequest.java com/validic/mobile/UserComponent.java com/validic/mobile/ValidicApiLogger.java com/validic/mobile/ValidicMobile.java com/validic/mobile/record/Record.java com/validic/mobile/shealth/SHealthDataParsers.java com/validic/mobile/shealth/SHealthManager.java com/validic/mobile/shealth/SHealthManagerImpl.java com/validic/mobile/shealth/SHealthObserverPr

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/validic/mobile/shealth/SHealthObserverProvider.java com/validic/mobile/shealth/SHealthResultParser.java com/validic/mobile/shealth/SHealthResultParserNutrition.java com/validic/mobile/shealth/SHealthService.java com/validic/mobile/shealth/SHealthSubscription.java edu/emory/mathcs/backport/java/util/concurrent/helpers/Utils.java lombok/bytecode/PoolConstantsApp.java lombok/bytecode/PostCompilerApp.java lombok/core/DiagnosticsReceiver.java lombok/core/Main.java lombok/core/PublicApiCreatorApp.java lombok/core/Version.java lombok/core/configuration/ConfigurationProblemReporter.java lombok/core/debug/FileLog.java lombok/core/debug/ProblemReporter.java lombok/core/runtimeDependencies/CreateLombokRuntimeApp.java lombok/delombok/Delombok.java lombok/delombok/DelombokApp.java lombok/eclipse/agent/MavenEcjBootstrapApp.java lombok/eclipse/handlers/EclipseSingularsRecipes.java lombok/installer/Installer.java lombok/javac/CompilerMessageSuppressor.java lombok/javac/JavacResolution.java lombok/javac/JavacTreeMaker.java lombok/patcher/ClassRootFinder.java lombok/patcher/ScriptManager.java lombok/patcher/Version.java lombok/permit/Permit.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseJavascriptAppInterfaceImpl.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/util/HLFileUtil.java lombok/installer/OsUtils.java lombok/javac/apt/Processor.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/l.java com/bumptech/glide/load/engine/p.java com/cerner/healthelife_android/BuildConfig.java com/cerner/healthelife_android/libraries/hlcommonslib/util/HLConstants.java com/cerner/healthelife_android/libraries/hlsettingslib/SettingsConstants.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/adapters/MessageDetailsDeserializer.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/model/MobileSiteDefNav.java com/cerner/healthelife_android/util/HealtheLifeUtil.java com/cerner/healthelife_android/util/ParsingAccessTokens.java com/newrelic/agent/android/harvest/AgentHealth.java com/newrelic/agent/android/harvest/HarvestConfiguration.java com/validic/mobile/record/Diabetes.java com/validic/mobile/record/Record.java org/jsoup/nodes/DocumentType.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/cerner/healthelife_android/firebaseNotifications/HLFireBaseMessagingService.java com/cerner/healthelife_android/util/LocalNotificationUtil.java com/newrelic/agent/android/util/Util.java edu/emory/mathcs/backport/java/util/Collections.java edu/emory/mathcs/backport/java/util/concurrent/ConcurrentSkipListMap.java lombok/core/debug/AssertionLogger.java org/jsoup/helper/DataUtil.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/cerner/consumer_mobile_sdk/service/RetrofitClient.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/service/RetrofitClient.java com/validic/mobile/UserComponent.java
6	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/cerner/healthelife_android/libraries/hlwebviewlibrary/adapters/DownloadDataAdapter.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/fragments/DownloadsFragment.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseJavascriptAppInterfaceImpl.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/util/MessageCacheHelperKt.java com/newrelic/agent/android/AndroidAgentImpl.java com/validic/common/BitmapUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/cerner/healthelife_android/libraries/hlwebviewlibrary/adapters/MobileSiteDefProfileNavMenuAdapter.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/adapters/ProfileNavMenuAdapter.java
8	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/cerner/consumer_mobile_sdk/BuildConfig.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/cerner/healthelife_android/libraries/hlbiometriccryptography/utils/BiometricCryptoOperator.java com/scottyab/aescrypt/AESCrypt.java
10	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/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseWebViewActivity.java
11	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/newrelic/agent/android/instrumentation/SQLiteInstrumentation.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/cerner/healthelife_android/libraries/hlwebviewlibrary/adapters/DownloadDataAdapter.java lombok/bytecode/PoolConstantsApp.java lombok/bytecode/PostCompilerApp.java lombok/core/PublicApiCreatorApp.java lombok/core/runtimeDependencies/CreateLombokRuntimeApp.java lombok/delombok/Delombok.java lombok/delombok/DelombokApp.java lombok/eclipse/agent/MavenEcjBootstrapApp.java lombok/installer/IdeLocation.java lombok/installer/InstallerGUI.java lombok/installer/OsUtils.java lombok/installer/eclipse/EclipseProductLocation.java lombok/installer/eclipse/EclipseProductLocationProvider.java lombok/javac/CapturingDiagnosticListener.java lombok/patcher/ScriptManager.java org/jsoup/Jsoup.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/cerner/healthelife_android/libraries/hldownloadmanagerlib/HLCalendarIntent.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/util/CacheHelper.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java com/validic/mobile/SessionData.java lombok/bytecode/PostCompilerApp.java lombok/core/configuration/ConfigurationFile.java lombok/delombok/Delombok.java lombok/installer/eclipse/EclipseProductLocation.java lombok/launch/d.java net/fortuna/ical4j/util/Calendars.java okio/c.java org/jsoup/helper/DataUtil.java org/threeten/bp/chrono/HijrahDate.java
00078	Get the network operator name	collection telephony	com/newrelic/agent/android/util/Connectivity.java
00033	Query the IMEI number	collection	com/newrelic/agent/android/util/PersistentUUID.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/newrelic/agent/android/harvest/HarvestConnection.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java org/jsoup/helper/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/crash/CrashSender.java com/newrelic/agent/android/harvest/HarvestConnection.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java org/jsoup/helper/HttpConnection.java
00096	Connect to a URL and set request method	command network	com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/harvest/HarvestConnection.java org/jsoup/helper/HttpConnection.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/cerner/consumer_mobile_sdk/restful/ConsumerSDKApiCallback.java com/cerner/healthelife_android/libraries/hldownloadmanagerlib/HLDownLoadListener.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseJavascriptAppInterfaceImpl.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseWebViewActivity.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/util/HLWebViewUtil.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/webclients/HLBaseWebViewClient.java com/cerner/healthelife_android/presenter/MainWebViewActivity.java com/cerner/healthelife_android/util/HealtheLifeUtil.java com/cerner/healthelife_android/util/PlayStoreInstance.java com/cerner/healthelife_android/webclients/LoginWebViewClient.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java com/validic/mobile/shealth/SHealthService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseJavascriptAppInterfaceImpl.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseWebViewActivity.java com/cerner/healthelife_android/libraries/hlwebviewlibrary/webclients/HLBaseWebViewClient.java com/cerner/healthelife_android/webclients/LoginWebViewClient.java
00108	Read the input stream from given URL	network command	com/newrelic/agent/android/harvest/HarvestConnection.java com/newrelic/agent/android/payload/PayloadSender.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00029	Initialize class object dynamically	reflection	lombok/eclipse/agent/EclipseLoaderPatcherTransplants.java
00046	Method reflection	reflection	lombok/eclipse/agent/EclipseLoaderPatcherTransplants.java
00202	Make a phone call	control	com/cerner/healthelife_android/libraries/hlwebviewlibrary/webclients/HLBaseWebViewClient.java
00203	Put a phone number into an intent	control	com/cerner/healthelife_android/libraries/hlwebviewlibrary/webclients/HLBaseWebViewClient.java
00094	Connect to a URL and read data from it	command network	com/newrelic/agent/android/harvest/HarvestConnection.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00091	Retrieve data from broadcast	collection	com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseWebViewActivity.java
00162	Create InetSocketAddress object and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/newrelic/agent/android/util/Reachability.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00024	Write file after Base64 decoding	reflection file	com/cerner/healthelife_android/libraries/hlwebviewlibrary/presenter/HLBaseJavascriptAppInterfaceImpl.java
00191	Get messages in the SMS inbox	sms	com/cerner/healthelife_android/libraries/hldownloadmanagerlib/HLDownLoadListener.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://vertical-vault-90315.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/130851680942/namespaces/firebase:fetch?key=AIzaSyDJXtcrmdJiE2T4vtDnY2k7V3RQ3uX8Tq4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_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
y.x	ok	No Geolocation information available.
dontcare.com	ok	**IP:** 23.227.38.32 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
projectlombok.org	ok	**IP:** 104.21.32.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
groups.google.com	ok	**IP:** 216.239.34.177 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mobile.validic.com	ok	**IP:** 18.189.97.193 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
iuhealth.consumermobile.us-1.healtheintent.com	ok	**IP:** 35.160.135.248 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
vertical-vault-90315.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
hub.samsungapps.com	ok	**IP:** 54.77.39.19 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
bujlqe0o.auth.us-west-2.amazoncognito.com	ok	**IP:** 35.165.221.175 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
x.y	ok	No Geolocation information available.
one-api-prod.avizia.com	ok	**IP:** 18.204.64.7 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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
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

EMAILS

EMAIL	FILE
kweiner@fmsware.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130

HARDCODED SECRETS

POSSIBLE SECRETS
"DEVICE_TOKEN" : "device_token"
"firebase_database_url" : "https://vertical-vault-90315.firebaseio.com"
"google_api_key" : "AIzaSyDJXtcrmdJiE2T4vtDnY2k7V3RQ3uX8Tq4"
"google_crash_reporting_api_key" : "AIzaSyDJXtcrmdJiE2T4vtDnY2k7V3RQ3uX8Tq4"
389C9738-A761-44DE-8A66-1668CFD67DA1
308204a830820390a003020102020900936eacbe07f201df300d06092a864886f70d01010505003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f69643110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303232393031333334365a170d3335303731373031333334365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f69643110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6931904dec60b24b1edc762e0d9d8253e3ecd6ceb1de2ff068ca8e8bca8cd6bd3786ea70aa76ce60ebb0f993559ffd93e77a943e7e83d4b64b8e4fea2d3e656f1e267a81bbfb230b578c20443be4c7218b846f5211586f038a14e89c2be387f8ebecf8fcac3da1ee330c9ea93d0a7c3dc4af350220d50080732e0809717ee6a053359e6a694ec2cb3f284a0a466c87a94d83b31093a67372e2f6412c06e6d42f15818dffe0381cc0cd444da6cddc3b82458194801b32564134fbfde98c9287748dbf5676a540d8154c8bbca07b9e247553311c46b9af76fdeeccc8e69e7c8a2d08e782620943f99727d3c04fe72991d99df9bae38a0b2177fa31d5b6afee91f020103a381fc3081f9301d0603551d0e04160414485900563d272c46ae118605a47419ac09ca8c113081c90603551d230481c13081be8014485900563d272c46ae118605a47419ac09ca8c11a1819aa48197308194310b300906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071307416e64726f69643110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900936eacbe07f201df300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100 7aaf968ceb50c441055118d0daabaf015b8a765a27a715a2c2b44f221415ffdace03095abfa42df70708726c2069e5c36eddae0400be29452c084bc27eb6a17eac9dbe182c204eb15311f455d824b656dbe4dc2240912d7586fe88951d01a8feb5ae5a4260535df83431052422468c36e22c2a5ef994d61dd7306ae4c9f6951ba3c12f1d1914ddc61f1a62da2df827f603fea5603b2c540dbd7c019c36bab29a4271c117df523cdbc5f3817a49e0efa60cbd7f74177e7a4f193d43f4220772666e4c4d83e1bd5a86087cf34f2dec21e245ca6c2bb016e683638050d2c430eea7c26a1c49d3760a58ab7f1a82cc938b4831384324bd0401fa12163a50570e684d
23456789abcdefghjkmnpqrstvwxyz
AAd875ba49ae6d327932372de9fd0da618fa4fca1a

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
f4c16537-aa0b-427f-8c31-3e466685cccd
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
308204d4308203bca003020102020900d20995a79c0daad6300d06092a864886f70d01010505003081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f7265613113301106035504071305375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d433115301306035504031305c53616d73756e672043657274312530230609a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531325a170d3338313130373132323531325a3081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f7265613113301106035504071305375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e672043657274312530230609a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100c986384a3e1f2fb206670e78ef232215c0d26f45a22728db99a44da11c35ac33a71fe071c4a2d6825a9b4c88b333ed96f3c5e6c666d60f3ee94c490885abcf8dc660f707aabc77ead3e2d0d8aee8108c15cd260f2e85042c28d2f292daa3c6da0c7bf2391db7841aade8fdf0c9d0defcf77124e6d2de0a9e0d2da746c3670e4ffcdc85b701bb4744861b96ff7311da3603c5a10336e55ffa34b4353eedc85f51015e1518c67e309e39f87639ff178107f109cd18411a6077f26964b6e63f8a70b9619db04306a323c1a1d23af867e19f14f570ffe573d0e3a0c2b30632aaec3173380994be1e341e3a90bd2e4b615481f46db39ea83816448ec35feb1735c1f3020103a382010b30820107301d0603551d0e04160414932c3af70b627a0c7610b5a0e7427d6cfaea3f1e3081d70603551d230481cf3081cc8014932c3af70b627a0c7610b5a0e7427d6cfaea3f1ea181a8a481a53081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e672043657274312530230609a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900d20995a79c0daad6300c0603551d13040530030101ff300d06092a864886f70d01010505000382010100329601fe40e036a4a86cc5d49dd8c1b5415998e72637538b0d430369ac51530f63aace8c019a1a66616a2f1bb2c5fabd6f313261f380e3471623f053d9e3c53f5fd6d1965d7b000e4dc244c1b27e2fe9a323ff077f52c4675e86247aa801187137e30c9bbf01c567a4299db4bf0b25b7d7107a7b81ee102f72ff47950164e26752e114c42f8b9d2a42e7308897ec640ea1924ed13abbe9d120912b62f4926493a86db94c0b46f44c6161d58c2f648164890c512dfb28d42c855bf470dbee2dab6960cad04e81f71525ded46cdd0f359f99c460db9f007d96ce83b4b218ac2d82c48f12608d469733f05a3375594669ccbf8a495544d6c5701e9369c08c810158

POSSIBLE SECRETS

308204a830820390a003020102020900b3998086d056cffa300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a436 16c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f696 43110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353232343 035305a170d3335303930313232343035305a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4 d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312 2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100 9 c780592ac0d5d381cdeaa65ecc8a6006e36480c6d7207b12011be50863aabe2b55d009adf7146d6f2202280c7cd4d7bdb26243b8a806c26b34b137523a49268224904dc 01493e7c0acf1a05c874f69b037b60309d9074d24280e16bad2a8734361951eaf72a482d09b204b1875e12ac98c1aa773d6800b9eafde56d58bed8e8da16f9a360099c37 a834a6dfedb7b6b44a049e07a269fccf2c5496f2cf36d64df90a3b8d8f34a3baab4cf53371ab27719b3ba58754ad0c53fc14e1db45d51e234fbbe93c9ba4edf9ce54261350e c535607bf69a2ff4aa07db5f7ea200d09a6c1b49e21402f89ed1190893aab5a9180f152e82f85a45753cf5fc19071c5eec827020103a381fc3081f9301d0603551d0e041604 144fe4a0b3dd9cba29f71d7287c4e7c38f2086c2993081c90603551d230481c13081be80144fe4a0b3dd9cba29f71d7287c4e7c38f2086c299a1819aa48197308194310b30 0906035504061302555331133011060355040813 0a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416 e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616 e64726f69642e636f6d820900b3998086d056cffa300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100572551b8d93a1f73de0f6d469f86d ad6701400293c88a0cd7cd778b73dafcc197fab76e6212e56c1c761cfc42fd733de52c50ae08814cefc0a3b5a1a4346054d829f1d82b42b2048bf88b5d14929ef85f60edd12 d72d55657e22e3e85d04c831d613d19938bb8982247fa321256ba12d1d6a8f92ea1db1c373317ba0c037f0d1aff645aef224979fba6e7a14bc025c71b98138cef3ddfc0596 17cf24845cf7b40d6382f7275ed738495ab6e5931b9421765c491b72fb68e080dbdb58c2029d347c8b328ce43ef6a8b15533edfbe989bd6a48dd4b202eda94c6ab8dd5b8 399203daae2ed446232e4fe9bd961394c6300e5138e3cfd285e6e4e483538cb8b1b357

POSSIBLE SECRETS
308204d4308203bca003020102020900e5eff0a8f66d92b3300d06092a864886f70d01010505003081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d301e170d3131303632323132323531335a170d3338313130373132323531335a3081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100e9f1edb42423201dce62e68f2159ed8ea766b43a43d348754841b72e9678ce6b03d06d31532d88f2ef2d5ba39a028de0857983cd321f5b7786c2d3699df4c0b40c8d856f147c5dc54b9d1d671d1a51b5c5364da36fc5b0fe825afb513ec7a2db862c48a6046c43c3b71a1e275155f6c30aed2a68326ac327f60160d427cf55b617230907a84edbff21cc256c628a16f15d55d49138cdf2606504e1591196ed0bdc25b7cc4f67b33fb29ec4dbb13dbe6f3467a0871a49e620067755e6f095c3bd84f8b7d1e66a8c6d1e5150f7fa9d95475dc7061a321aaf9c686b09be23ccc59b35011c6823ffd5874d8fa2a1e5d276ee5aa381187e26112c7d5562703b36210b020103a382010b30820107301d0603551d0e041604145b115b23db35655f9f77f78756961006eebe3a9e3081d70603551d230481cf3081cc80145b115b23db35655f9f77f78756961006eebe3a9ea181a8a481a53081a2310b3009060355040613024b52311430120603550408130b536f757468204b6f726561311330110603550407130a5375776f6e2043697479311c301a060355040a131353616d73756e6720436f72706f726174696f6e310c300a060355040b1303444d43311530130603550403130c53616d73756e6720436572743125302306092a864886f70d0109011616616e64726f69642e6f734073616d73756e672e636f6d820900e5eff0a8f66d92b3300c0603551d13040530030101ff300d06092a864886f70d0101050500038201010039c91877eb09c2c84445443673c77a1219c5c02e6552fa2fbad0d736bc5ab6ebaf0375e520fe9799403ecb71659b23afda1475a34ef4b2e1ffcba8d7ff385c21cb6482540bce3837e6234fd4f7dd576d7fcfe9cfa925509f772c494e1569fe44e6fcd4122e483c2caa2c639566dbcfe85ed7818d5431e73154ad453289fb56b607643919cf534fbeefbdc2009c7fcb5f9b1fa97490462363fa4bedc5e0b9d157e448e6d0e7cfa31f1a2faa9378d03c8d1163d3803bc69bf24ec77ce7d559abcaf8d345494abf0e3276f0ebd2aa08e4f4f6f5aaea4bc523d8cc8e2c9200ba551dd3d4e15d5921303ca9333f42f992ddb70c2958e776c12d7e3b7bd74222eb5c7a
01360240043788015936020505
308201e53082014ea00302010202044f54468b300d06092a864886f70d01010505003037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d3132303330353034353232375a170d3432303232363034353232375a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f696420446562756730819f300d06092a864886f70d010101050003818d00308189028181008a53be36d02befe1d152724281630bd1c42eff0edf5fdca8eb944f536ab3f54dca9b22cfb421b37706a4ad259101815723202b359250cf6c59905032798273462bfa3f9f1881f7475ee5b25849edefac81085815f42383a44cb2be1bfd5c1f049ef42f5818f35fe0b1131c769cee347d558395a5fa87c3d425b2b9c819cf91870203010001300d06092a864886f70d0101050500038181000512992268a01e0941481931f3f9b6647fbe25ee0bc9648f35d56c55f8cfa6c935fb3d435125fd60ef566769ac7e64fe2823409461ca7a04570c43baaab3fb877bf3a6a8dd9ef7e69944f65b0e5e36f2ac2bf085fdeda063898855ea2ce84c60655d824844fe1659a77c12604c3fb84d41df6f1a7705a1b9962ac2fdc9933122
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb

PLAYSTORE INFORMATION

Title: My IU Health

Score: 4.145161 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.iuhealth.healthelife.play

Developer Details: Indiana University Health, Indiana+University+Health, None, None, webmaster@iuhealth.org,

Release Date: Jul 8, 2024 **Privacy Policy:** Privacy link

Description:

With My IU Health, you can self-schedule appointments with select providers, pay a bill, send secure messages to your care team, access medical records, view lab reports and manage prescription renewals. Participating providers can also allow you to add your HealthKit data to your electronic medical record.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 15:20:27	Generating Hashes	OK
2025-09-01 15:20:27	Extracting APK	OK
2025-09-01 15:20:27	Unzipping	OK
2025-09-01 15:20:34	Parsing APK with androguard	OK
2025-09-01 15:20:34	Extracting APK features using aapt/aapt2	OK

2025-09-01 15:20:34	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 15:20:37	Parsing AndroidManifest.xml	OK
2025-09-01 15:20:37	Extracting Manifest Data	OK
2025-09-01 15:20:37	Manifest Analysis Started	OK
2025-09-01 15:20:38	Reading Network Security config from network_security_config.xml	OK
2025-09-01 15:20:38	Parsing Network Security config	OK
2025-09-01 15:20:38	Performing Static Analysis on: My IU Health (org.iuhealth.healthelife.play)	OK
2025-09-01 15:20:39	Fetching Details from Play Store: org.iuhealth.healthelife.play	OK
2025-09-01 15:20:42	Checking for Malware Permissions	OK
2025-09-01 15:20:42	Fetching icon path	OK

2025-09-01 15:20:42	Library Binary Analysis Started	OK
2025-09-01 15:20:47	Reading Code Signing Certificate	OK
2025-09-01 15:20:47	Running APKiD 2.1.5	OK
2025-09-01 15:20:51	Detecting Trackers	OK
2025-09-01 15:20:54	Decompiling APK to Java with JADX	OK
2025-09-01 15:21:17	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 15:21:17	Decompiling classes2.dex with JADX	OK
2025-09-01 15:21:25	Decompiling classes.dex with JADX	OK
2025-09-01 15:21:34	Decompiling classes2.dex with JADX	OK
2025-09-01 15:21:42	Decompiling classes.dex with JADX	OK

2025-09-01 15:21:52	Converting DEX to Smali	OK
2025-09-01 15:21:52	Code Analysis Started on - java_source	OK
2025-09-01 15:21:56	Android SBOM Analysis Completed	OK
2025-09-01 15:22:01	Android SAST Completed	OK
2025-09-01 15:22:01	Android API Analysis Started	OK
2025-09-01 15:22:07	Android API Analysis Completed	OK
2025-09-01 15:22:07	Android Permission Mapping Started	OK
2025-09-01 15:22:13	Android Permission Mapping Completed	OK
2025-09-01 15:22:13	Android Behaviour Analysis Started	OK
2025-09-01 15:22:19	Android Behaviour Analysis Completed	OK
2025-09-01 15:22:19	Extracting Emails and URLs from Source Code	OK

2025-09-01 15:22:22	Email and URL Extraction Completed	OK
2025-09-01 15:22:22	Extracting String data from APK	OK
2025-09-01 15:22:22	Extracting String data from Code	OK
2025-09-01 15:22:22	Extracting String values and entropies from Code	OK
2025-09-01 15:22:27	Performing Malware check on extracted domains	OK
2025-09-01 15:22:29	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.