ANDROID STATIC ANALYSIS REPORT

Marathon Health (2024.11)

File Name:	com.marathonhealth.app_26186.apk
Package Name:	com.marathonhealth.app
Scan Date:	Aug. 31, 2025, 2:23 a.m.
App Security Score:	58/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	15	3	3	1

FILE INFORMATION

File Name: com.marathonhealth.app_26186.apk

Size: 28.52MB

MD5: fd23a15af8986f2792ce3462aea37a06

SHA1: dec117c972210c27924c4fac953cb79cc59b11dd

SHA256: 0d3bd556f4f0e5298b2825f4b0b9a839d894e136b369df33cc05451017493ecb

APP INFORMATION

App Name: Marathon Health

Package Name: com.marathonhealth.app

Main Activity: com.mma.android.screens.login.ui.LoginActivity

Target SDK: 34

Min SDK: 29

Max SDK:

Android Version Name: 2024.11

Android Version Code: 26186

APP COMPONENTS

Activities: 21
Services: 13
Receivers: 12
Providers: 3
Exported Activities: 4
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, CN=Marathon Health
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-22 19:57:07+00:00
Valid To: 2045-12-16 19:57:07+00:00
Issuer: C=US, CN=Marathon Health
Serial Number: 0x91e83b4
Hash Algorithm: sha256
md5: 06b7a3dc74c97015ee430d54cf16a913
sha1: 985e6e81f6b668a92ce69cc258150bd64a07c74e
sha256: b3e619e4f8da0dd07f1c28a64c343df0fd1e29d8292a1ea3557a649e897d6482
sha512: 49c961c91eb74cc73b7f0aae67286d0243f75e685a410590ae02b8477a8a9e7b85d652e3fa7f18a2a5700985eb2cb601c6a0a219fd15ebbb0254b8abcd58d087
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4e4f3b6f8a00059f22669b57c66a98ea02c1d1e45fcd808b8b60a8603d5ea8d8
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.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.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.

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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.marathonhealth.app.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>fd23a15af8986f2792ce3462aea37a06.apk</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table></td></tr>
<tr><td>classes.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.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>
</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.MANUFACTURER check
Build.TAGS 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>Anti-VM Code</td><td>Build.MANUFACTURER check
possible Build.SERIAL check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mma.android.screens.login.ui.LoginActivity	Schemes: @string/base_browsable_marathon_health_scheme://, Hosts: @string/browsable_marathon_health_host_visit_appointments,
com.mma.android.screens.home.ui.HomeActivity	Schemes: @string/base_browsable_marathon_health_scheme://, Hosts: @string/base_browsable_marathon_health_host_appointments, @string/base_browsable_marathon_health_host_validic_devices,

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: **8** | 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.mma.android.screens.home.ui.HomeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	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.
5	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
6	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.
7	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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.
9	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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.

CODE ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b2/c.java c/c.java c0/a.java c0/b.java c0/d.java com/aliumujib/swipetorefresh/SwipeToRefreshLayout.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 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/d.java com/bumptech/glide/load/engine/executor/GlideE

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xecutor.java com/bumptech/glide/load/engine/h.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/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.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.jav

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	a com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/b.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/mma/android/MarathonApplication.java com/mma/android/core/domain/models/biometric/BiometricSupport.java com/mma/android/core/domain/repositories/biometric/BiometricCryptoRepository.java com/mma/android/core/extensions/ContextExtensionsKt.java com/mma/android/core/presentation/helpers/BiometricPromptUtils.java com/mma/android/incentives/domain/useCases/validicConnection/ValicConnectionManagerImpl.java com/mma/android/incentives/presentation/helpers/GoogleFitConnectionManager.java com/mma/android/incentives/presentation/screens/devices/ui/AddDeviceFragment.java com/mma/android/incentives/presentation/screens/devices/viewmodel/DevicesConnectionViewModel.java com/mma/android/incentives/presentation/screens/status/adapter/IncentiveGoalAdapter.java com/mma/android/incentives/presentation/screens/status/ui/IncentivesLandingPageFragment.java com/mma/android/incentives/presentation/screens/status/viewmodel/IncentivesViewModel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mma/android/incentives/presentation/screens/summary/viewmodel/MySummaryViewModel.java com/mma/android/screens/appointments/home/viewmodel/AppointmentsHomeViewModel.java com/mma/android/screens/externallink/ExternalLinkUtils.java com/mma/android/screens/login/viewmodel/LoginViewModel$callApiSignIn$1.java com/mma/android/screens/login/viewmodel/LoginViewModel.java com/mma/android/screens/more/viewmodel/MoreViewModel.java com/mma/android/screens/myhealth/viewmodel/MyHealthFragmentViewModel.java com/mma/android/utils/InAppReviewManager.java com/mma/android/utils/SingleLiveEvent.java com/validic/common/BitmapUtil.java com/validic/mobile/AppModule.java com/validic/mobile/MediaWorker.java com/validic/mobile/MultiRecordRequest.java com/validic/mobile/RecordWorker.java com/validic/mobile/Session.java com/validic/mobile/SessionDataFileSerializer.java com/validic/mobile/SessionImpl.java com/validic/mobile/SessionStorageImpl.java com/validic/mobile/SingleRecordRequest.java com/validic/mobile/ValidateCredentialsWorker.java com/validic/mobile/ValidicApiLogger.java com/validic/mobile/ValidicMobile.java com/validic/mobile/WorkManagerQueue.java com/validic/mobile/aggregator/fit/FitAggregatorDelegate.java com/validic/mobile/aggregator/fit/GoogleFitReceiver.java com/validic/mobile/aggregator/fit/ValidicFitManager.java com/validic/mobile/record/Record.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dagger/android/AndroidInjection.java e/e.java io/freshpaint/android/integrations/Logger.java io/noties/markwon/LinkResolverDef.java io/noties/markwon/PrecomputedTextSetterCompat.java j/v.java junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java m/d.java m2/c.java m2/d.java m2/f.java n2/c.java n2/k.java n2/o.java n2/q.java net/nightwhistler/htmlspanner/SpanStack.java net/nightwhistler/htmlspanner/SystemFontResolver.java net/nightwhistler/htmlspanner/css/CSSCompiler.java net/nightwhistler/htmlspanner/handlers/StyleNodeHandler.java net/nightwhistler/htmlspanner/handlers/StyledTextHandler.java net/nightwhistler/htmlspanner/handlers/attributes/BorderAttributeHandler.java net/nightwhistler/htmlspanner/handlers/attributes/StyleAttributeHandler.java net/nightwhistler/htmlspanner/spans/BorderSpan.java net/nightwhistler/htmlspanner/style/StyleCallback.java net/nightwhistler/htmlspanner/style/StyleValue.java o1/c.java o5/b.java org/htmlcleaner/CommandLine.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/htmlcleaner/ConfigFileTagProvider.java org/mockito/internal/debugging/MockitoDebuggerImpl.java org/mockito/internal/util/ConsoleMockitoLogger.java p3/a.java q5/b0.java q5/e0.java q5/g0.java q5/l0.java q5/m0.java q5/n0.java q5/o0.java q5/q0.java q5/r0.java s1/a.java s2/e.java t1/a.java t5/a.java u0/d.java u1/a.java
2	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	c/c.java
3	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	aa/e.java ca/h.java org/junit/rules/TemporaryFolder.java org/mockito/internal/creation/bytebuddy/InlineByteBuddyMockMaker.java
				com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/f.java com/mma/android/core/helpers/CoreConstants.java com/mma/android/di/AppointmentManager.java com/mma/android/incentives/helpers/IncentivesConstants.java com/mma/android/incentives/presentation/screens/hra/HRABaseFragment.java com/mma/android/network/pojo/flippers/Flippers

NO	ISSUE	SEVERITY	STANDARDS	FILES
				.java com/mma/android/network/pojo/flippers/FlippersAttributes.java
4	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/mma/android/screens/appointments/home/ui/fragment/AppointmentDetailFragment.java com/mma/android/screens/appointments/scheduling/presentation/ui/choosetime/dialog/NetworkProviderDialog.java com/mma/android/screens/appointments/scheduling/presentation/ui/choosetime/dialog/TimeChooseConfirmationDialog.java com/mma/android/screens/messaging/ui/MessageNotSentErrorDialog.java com/mma/android/screens/messaging/ui/MessageThreadFragment.java com/mma/android/screens/messaging/ui/NewMessageFragment.java com/mma/android/screens/signup/data/models/signUpVerify/SignUpAttributes.java com/validic/mobile/V1ApiService.java com/validic/mobile/WorkManagerQueue.java com/validic/mobile/aggregator/fit/DataParser.java com/validic/mobile/aggregator/fit/FitAggregatorDelegate.java com/validic/mobile/aggregator/fit/SummaryWorker.java com/validic/mobile/record/Diabetes.java com/validic/mobile/record/Record.java io/freshpaint/android/Options.java p1/b.java p1/i.java
5	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/annimon/stream/RandomCompat.java fa/a.java org/junit/runner/manipulation/Ordering.java org/mockito/internal/creation/bytebuddy/a.java u9/i.java u9/k.java z5/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/mma/android/di/RetrofitModule.java com/validic/mobile/AppModule.java
7	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/validic/common/BitmapUtil.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/validic/mobile/aggregator/fit/FitAggregatorDelegate.java com/validic/mobile/auth/LicenseManager.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/mma/android/core/domain/repositories/biometric/BiometricCryptoRepository.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	q5/b0.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	aa/c.java aa/e.java c5/k.java 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/mma/android/screens/externallink/ExternalLinkUtils.java com/validic/mobile/SessionDataFileSerializer.java d5/d.java junit/runner/BaseTestRunner.java okio/d.java org/htmlcleaner/HtmlCleaner.java org/junit/experimental/max/MaxHistory.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/mma/android/core/extensions/ContextExtensionsKt.java com/mma/android/core/helpers/PhoneUtils.java com/mma/android/screens/appointments/home/viewmodel/AppointmentDetailViewModel.java com/mma/android/screens/messaging/ui/MessageBaseFragment.java com/mma/android/screens/messaging/ui/MessageThreadFragment.java com/mma/android/ui/BaseView.java io/noties/markwon/LinkResolverDef.java
00014	Read file into a stream and put it into a JSON object	file	d5/d.java
00022	Open a file from given absolute path of the file	file	com/mma/android/screens/externallink/presentation/ExternalLinkFragment.java com/mma/android/screens/messaging/ui/MessageBaseFragment.java d5/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	d5/d.java
00096	Connect to a URL and set request method	command network	io/freshpaint/android/ConnectionFactory.java y1/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java y1/c.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java y1/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	c0/d.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00033	Query the IMEI number	collection	io/freshpaint/android/AnalyticsContext.java io/freshpaint/android/internal/Utils.java
00036	Get resource file from res/raw directory	reflection	io/noties/markwon/LinkResolverDef.java
00187	Query a URI and check the result	collection sms calllog calendar	c0/d.java
00202	Make a phone call	control	com/mma/android/core/helpers/PhoneUtils.java
00203	Put a phone number into an intent	control	com/mma/android/core/helpers/PhoneUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/mma/android/core/helpers/PhoneUtils.java com/mma/android/screens/messaging/ui/MessageBaseFragment.java
00091	Retrieve data from broadcast	collection	com/mma/android/screens/home/ui/HomeActivity.java
00125	Check if the given file path exist	file	com/mma/android/screens/messaging/ui/MessageBaseFragment.java
00191	Get messages in the SMS inbox	sms	com/mma/android/screens/messaging/ui/MessageBaseFragment.java
00078	Get the network operator name	collection telephony	io/freshpaint/android/AnalyticsContext.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/547464326582/namespaces/firebase:fetch?key=AIzaSyBkYOWrzfwcBlMsrkckbBIF0i_829wrhWk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.CALL_PHONE, android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, 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

DOMAIN	STATUS	GEOLOCATION
jdom.org	ok	**IP:** 204.13.10.92 **Country:** United States of America **Region:** Oregon **City:** Corvallis **Latitude:** 44.517742 **Longitude:** -123.298096 **View:** Google Map
android.asset	ok	No Geolocation information available.
s3.amazonaws.com	ok	**IP:** 16.15.189.112 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.409912 **Longitude:** -122.160400 **View:** Google Map
mobile.marathon-health.com	ok	**IP:** 98.86.205.235 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
search.maven.org	ok	**IP:** 3.211.174.179 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
syncmydevice.com	ok	**IP:** 76.223.2.138 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
mobile.validic.com	ok	**IP:** 3.128.169.119 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
my.marathon-health.comssjump	ok	No Geolocation information available.
mobile-service.segment.com	ok	No Geolocation information available.
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
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
my.marathon-health.coms	ok	No Geolocation information available.
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
api.perfalytics.com	ok	**IP:** 18.155.173.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	n2/j.java

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" : "eb250b92773e4f348d84a989afa78007"
"google_api_key" : "AIzaSyBkYOWrzfwcBlMsrkckbBIF0i_829wrhWk"
"google_crash_reporting_api_key" : "AIzaSyBkYOWrzfwcBlMsrkckbBIF0i_829wrhWk"
"password" : "Password"
"provider_authorities" : "com.marathonhealth.app.fileprovider"
"username" : "Username"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
ae66152b-60be-4809-a73c-96eefd2c357d
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
9fc27524-d828-4fb6-8e87-9c89ce10dd67
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

POSSIBLE SECRETS
cd889f08-8cfb-4d31-b3d6-dbca6a09b0fd

PLAYSTORE INFORMATION

Title: Marathon Health

Score: 3.54 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.marathonhealth.app

Developer Details: Marathon Health, Marathon+Health, None, https://marathon.health, AppSupport@marathon-health.com,

Release Date: Jun 17, 2021 **Privacy Policy:** Privacy link

Description:

Our patient portal and app are always available, so you can access your health records, message your care team, view lab results, and request refills on your schedule, 24/7.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 02:23:30	Generating Hashes	OK
2025-08-31 02:23:30	Extracting APK	OK
2025-08-31 02:23:30	Unzipping	OK

2025-08-31 02:23:30	Parsing APK with androguard	OK
2025-08-31 02:23:31	Extracting APK features using aapt/aapt2	OK
2025-08-31 02:23:31	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 02:23:39	Parsing AndroidManifest.xml	OK
2025-08-31 02:23:39	Extracting Manifest Data	OK
2025-08-31 02:23:39	Manifest Analysis Started	OK
2025-08-31 02:23:39	Reading Network Security config from network_security_config.xml	OK
2025-08-31 02:23:39	Parsing Network Security config	OK
2025-08-31 02:23:39	Performing Static Analysis on: Marathon Health (com.marathonhealth.app)	OK
2025-08-31 02:23:39	Fetching Details from Play Store: com.marathonhealth.app	OK
2025-08-31 02:23:39	Checking for Malware Permissions	OK

2025-08-31 02:23:39	Fetching icon path	OK
2025-08-31 02:23:39	Library Binary Analysis Started	OK
2025-08-31 02:23:40	Reading Code Signing Certificate	OK
2025-08-31 02:23:40	Running APKiD 2.1.5	OK
2025-08-31 02:23:42	Detecting Trackers	OK
2025-08-31 02:23:47	Decompiling APK to Java with JADX	OK
2025-08-31 02:30:27	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-31 02:30:27	Decompiling classes2.dex with JADX	OK
2025-08-31 02:30:44	Decompiling classes4.dex with JADX	OK
2025-08-31 02:30:52	Decompiling classes.dex with JADX	OK
2025-08-31 02:31:20	Decompiling classes3.dex with JADX	OK

2025-08-31 02:31:37	Decompiling classes2.dex with JADX	OK
2025-08-31 02:31:49	Decompiling classes4.dex with JADX	OK
2025-08-31 02:31:53	Decompiling classes.dex with JADX	OK
2025-08-31 02:32:06	Decompiling classes3.dex with JADX	OK
2025-08-31 02:32:24	Converting DEX to Smali	OK
2025-08-31 02:32:24	Code Analysis Started on - java_source	OK
2025-08-31 02:32:35	Android SBOM Analysis Completed	OK
2025-08-31 02:32:48	Android SAST Completed	OK
2025-08-31 02:32:48	Android API Analysis Started	OK
2025-08-31 02:33:28	Android API Analysis Completed	OK
2025-08-31 02:33:28	Android Permission Mapping Started	OK

2025-08-31 02:34:03	Android Permission Mapping Completed	OK
2025-08-31 02:34:22	Android Behaviour Analysis Started	OK
2025-08-31 02:34:37	Android Behaviour Analysis Completed	OK
2025-08-31 02:34:37	Extracting Emails and URLs from Source Code	OK
2025-08-31 02:34:56	Email and URL Extraction Completed	OK
2025-08-31 02:34:56	Extracting String data from APK	OK
2025-08-31 02:34:56	Extracting String data from Code	OK
2025-08-31 02:34:56	Extracting String values and entropies from Code	OK
2025-08-31 02:35:22	Performing Malware check on extracted domains	OK
2025-08-31 02:35:29	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.