ANDROID STATIC ANALYSIS REPORT

MyHealthONE (1.4.36)

File Name:	com.hcahealthcare.mhom_1004036.apk
Package Name:	com.hcahealthcare.mhom
Scan Date:	Aug. 29, 2025, 11:30 p.m.
App Security Score:	64/100 (LOW RISK)
Grade:	A
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
0	16	4	4	1

FILE INFORMATION

File Name: com.hcahealthcare.mhom_1004036.apk
Size: 29.2MB
MD5: 25033e87c9e96ed3d8024f11bf206be9
SHA1: abe75b80ea7cb9f96b1a36371e22840373acb02a
SHA256: e37b010a00967b65b58f624aa9bb74577ac665b764bbe38f9f3a2f3bcef428e1

APP INFORMATION

App Name: MyHealthONE
Package Name: com.hcahealthcare.mhom
Main Activity: com.hcahealthcare.mhom.feature.splash.activity.StartActivity
Target SDK: 34
Min SDK: 31
Max SDK:
Android Version Name: 1.4.36

Android Version Code: 1004036

APP COMPONENTS

Activities: 19
Services: 14
Receivers: 12
Providers: 2
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=1, ST=Tennessee, L=Nashville, O=HCA, OU=ITG, CN=Travis Smith
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-14 17:14:25+00:00
Valid To: 2044-11-07 17:14:25+00:00
Issuer: C=1, ST=Tennessee, L=Nashville, O=HCA, OU=ITG, CN=Travis Smith
Serial Number: 0x445c48b2
Hash Algorithm: sha256
md5: 626d2df04bc2940a36f7624210e6462d
sha1: ced0391e0cc8bbe3fc432602f038d645614ed3c3
sha256: 1525d3ec5cbe2c751a46745b2f829db5f18ec25151add1df139156c87115f559
sha512: 3fa5c8b88f81738aec5020e6e49882fb3f900119b390d2971c5285c428469bfdf0717e3d0a90adc6729eca4889d622408089bb98da2147fc613bee31c31ae032
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5fed0cdd758896d30ad1cdc272d5faf0976738b182f2cae84d7952bb25434034
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.hcahealthcare.mhom.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	crm.hcaservices.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: IvsUVhycZdOvidhiv8pAezjM29PzY+IAUrxLHyy4srk= Digest: SHA-256,Pin: OSqnIRIhJQGKEtc7abZMpS4Y3djh39opzqI2WqlYVqM= Digest: SHA-256]

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: **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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
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.

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: **0** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/s0.java ab/a.java b2/b.java bb/d.java c3/l.java com/airbnb/lottie/LottieAnimationView.java com/hcahealthcare/mhom/base/c0.java com/hcahealthcare/mhom/feature/account/fragment/AccountFragment.java com/hcahealthcare/mhom/feature/login/fragment/ForgotPasswordFragment.java com/hcahealthcare/mhom/feature/profile/fragment/EditProfileFragment.java com/hcahealthcare/mhom/feature/splash/activity/StartActivity.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck3/LicenseClientV3.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va com/pdfview/subsamplincscaleimageview/decoder/SkiaPooledImageRegionDecoder.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java dq/q.java e/d.java e2/a.java eb/g.java ec/b.java el/a.java el/j.java el/k.java el/m.java f1/d.java f5/e.java fc/c.java fl/a.java h9/a.java h9/b.java h9/c.java i1/h.java j0/a0.java j2/c.java j5/a.java ja/a.java jl/c.java k2/a.java k9/b.java k9/c.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	k9/d.java k9/h.java k9/i.java k9/r.java k9/s.java k9/t.java ka/a.java l/c.java l0/d.java l2/a.java l9/d0.java l9/e.java l9/h.java l9/i.java l9/i0.java l9/l.java l9/u.java l9/y.java lb/p.java ml/a.java n1/c.java n9/a0.java na/i.java nl/i0.java o2/c.java o4/c.java o9/a.java o9/c.java o9/c0.java o9/f1.java o9/i1.java o9/s0.java o9/v0.java o9/w0.java o9/x0.java o9/z.java o9/z0.java ob/i.java p/d.java p/e.java p/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p/h.java p/i.java p/k.java p/l.java q2/o.java q2/r.java q2/u.java q2/y.java s2/a.java s9/a.java sb/g.java sb/o.java t0/d.java t9/f.java t9/m.java t9/n.java tc/a.java tp/c.java u2/h.java u4/g.java v0/c.java v0/o.java v2/d.java vi/a0.java w2/a.java w5/a.java x0/f.java x2/a.java x7/f.java x8/k.java x9/b.java y/m0.java z0/a.java z0/c.java z0/d.java z0/f.java z8/a.java zh/a.java
				be/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	be/f.java com/hcahealthcare/mhom/feature/account/model/AccountSwitchOverlayDataModel.java com/hcahealthcare/mhom/feature/profile/model/ProfileDataModel.java com/hcahealthcare/mhom/feature/profile/model/RelationshipModel.java com/hcahealthcare/mhom/feature/records/conditions/model/ConditionArticleModel.java com/hcahealthcare/mhom/feature/records/healthrecords/fragment/p1.java com/hcahealthcare/mhom/feature/records/healthrecords/fragment/w1.java com/hcahealthcare/mhom/feature/records/medications/model/MedicationArticleModel.java com/hcahealthcare/mhom/feature/sharerecord/model/ShareDocumentModel.java de/a.java fh/a.java gk/a.java gk/b.java gk/c.java gk/d.java gk/h.java h3/d.java ig/a.java ji/b.java ke/c.java md/b0.java md/k.java me/d.java me/e.java me/f.java me/g.java ne/a.java ne/e.java ne/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ne/h.java nl/e0.java nl/t0.java ph/d.java si/z0.java u3/c.java ul/g.java w3/m.java yh/q.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	s4/b.java sp/c.java sp/d.java sp/g.java sp/h.java
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	ig/b.java ip/z.java jo/a.java jo/b.java ko/a.java wp/d.java wp/h.java x4/a.java x4/b.java
5	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	l4/g.java r7/b.java
6	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	a0/u.java ec/c.java q2/y.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	d9/b0.java d9/h0.java m7/a.java n7/a.java v2/c.java y4/c.java y4/e.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	ll/a.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/hcahealthcare/mhom/util/PhotoHelper.java com/yalantis/ucrop/util/FileUtils.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	lb/c.java ll/b.java ob/v.java q4/w.java
11	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/hcahealthcare/mhom/component/FpWebView.java
12	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	fl/y.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	nl/x0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	ec/b.java
15	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	u1/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	a0/u.java c4/r.java com/hcahealthcare/mhom/util/PhotoHelper.java j7/a.java l4/g.java l4/h.java o3/a.java q2/y.java v2/d.java w2/a.java
00096	Connect to a URL and set request method	command network	d6/f.java fc/c.java l4/b.java
00089	Connect to a URL and receive input stream from the server	command network	d6/f.java r4/a.java
00109	Connect to a URL and get the response code	network command	d6/f.java r4/a.java
00153	Send binary data over HTTP	http	d6/f.java
00075	Get location of the device	collection location	nl/d.java
00137	Get last known location of the device	location collection	nl/d.java
00115	Get last known location of the device	collection location	nl/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a0/u.java com/yalantis/ucrop/util/FileUtils.java da/f.java ec/c.java l4/g.java l4/h.java p001do/g.java q2/y.java s2/b.java yp/x.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/hcahealthcare/mhom/base/c0.java com/hcahealthcare/mhom/feature/care/fragment/CareMenuFragment.java com/hcahealthcare/mhom/feature/records/medicalrecordslinking/fragments/MedicalRecordNotLinkedFragment.java com/hcahealthcare/mhom/feature/settings/fragment/SettingsFragment.java com/hcahealthcare/mhom/feature/splash/activity/StartActivity.java com/hcahealthcare/mhom/feature/visits/fragment/VisitsFragment.java el/i.java fl/a.java fl/d0.java fl/j.java l9/f.java
00202	Make a phone call	control	fl/a.java fl/d0.java
00203	Put a phone number into an intent	control	fl/a.java fl/d0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/hcahealthcare/mhom/feature/care/fragment/CareMenuFragment.java com/hcahealthcare/mhom/feature/records/medicalrecordslinking/fragments/MedicalRecordNotLinkedFragment.java com/hcahealthcare/mhom/feature/visits/fragment/VisitsFragment.java el/i.java fl/a.java fl/d0.java fl/j.java l9/f.java
00036	Get resource file from res/raw directory	reflection	com/hcahealthcare/mhom/feature/login/fragment/LauncherFragment.java com/hcahealthcare/mhom/feature/settings/fragment/SettingsFragment.java fl/j.java jl/c.java l9/f.java t3/e.java
00091	Retrieve data from broadcast	collection	com/hcahealthcare/mhom/feature/dashboard/activity/DashboardActivity.java com/hcahealthcare/mhom/feature/onboarding/OnboardingActivity.java
00012	Read data and put it into a buffer stream	file	da/f.java
00079	Hide the current app's icon	evasion	i3/l.java
00024	Write file after Base64 decoding	reflection file	c4/r.java
00030	Connect to the remote server through the given URL	network	l4/b.java
00112	Get the date of the calendar event	collection calendar	yc/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	e5/a.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/hcahealthcare/mhom/util/PhotoHelper.java
00029	Initialize class object dynamically	reflection	f2/w.java
00162	Create InetSocketAddress object and connecting to it	socket	sp/b.java sp/h.java
00163	Create new Socket and connecting to it	socket	sp/b.java sp/h.java
00114	Create a secure socket connection to the proxy address	network command	np/f.java
00161	Perform accessibility service action on accessibility node info	accessibility service	i1/h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	i1/h.java
00192	Get messages in the SMS inbox	sms	com/yalantis/ucrop/util/FileUtils.java
00014	Read file into a stream and put it into a JSON object	file	ec/c.java
00130	Get the current WIFI information	wifi collection	nl/b1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://mho-native.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/41696609448/namespaces/firebase:fetch?key=AIzaSyDI_FzMuBF-uh454cHEhlCyd0tRqkNul1c. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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
api.external.medcity.net	ok	**IP:** 165.214.41.240 **Country:** United States of America **Region:** Tennessee **City:** Nashville **Latitude:** 36.155300 **Longitude:** -86.789101 **View:** Google Map
aka.ms	ok	**IP:** 23.45.41.245 **Country:** United States of America **Region:** California **City:** El Segundo **Latitude:** 33.919182 **Longitude:** -118.416473 **View:** Google Map
dc.secure.ehc.com	ok	**IP:** 34.160.237.90 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
classevent.myhealthone.com	ok	**IP:** 165.214.41.39 **Country:** United States of America **Region:** Tennessee **City:** Nashville **Latitude:** 36.155300 **Longitude:** -86.789101 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mho-native.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
hcahealthcare.com	ok	**IP:** 13.107.246.69 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
bf28165iqg.bf.dynatrace.com	ok	**IP:** 54.165.26.183 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sandbox.swellbox.com	ok	**IP:** 54.144.131.221 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 64.233.176.157 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
oas.myhealthone.com	ok	**IP:** 165.214.41.39 **Country:** United States of America **Region:** Tennessee **City:** Nashville **Latitude:** 36.155300 **Longitude:** -86.789101 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
myhealthone.com	ok	**IP:** 199.91.39.113 **Country:** United States of America **Region:** Tennessee **City:** Nashville **Latitude:** 36.155300 **Longitude:** -86.789101 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.myhealthone.net	ok	**IP:** 199.91.39.113 **Country:** United States of America **Region:** Tennessee **City:** Nashville **Latitude:** 36.155300 **Longitude:** -86.789101 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **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	l9/t.java
mhotest1@hcadmp-staging.direct myhealthone@mho.staging	fk/c.java

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"app_file_provider_authority" : "com.hcahealthcare.mhom.fileprovider"
"firebase_database_url" : "https://mho-native.firebaseio.com"
"google_api_key" : "AIzaSyDI_FzMuBF-uh454cHEhlCyd0tRqkNul1c"
"google_crash_reporting_api_key" : "AIzaSyDI_FzMuBF-uh454cHEhlCyd0tRqkNul1c"
"password" : "Password"
"username" : "Username"
FSXT7Fy+LHUaRnRbL4KdtfGOwlFRrdHfE5FWyHEV9Vk=
sbtox8THdGaThdsCRhkAGyMU2V5wJ5vW
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
c0312754-776b-4c5a-8a39-7a77ea651d5a

POSSIBLE SECRETS
cHJvZC1leHRlcm5hbF9zYnRveDhUSGRHYVRoZHNDUmhrQUd5TVUyVjV3SjV2VzpmWFNGUHpxdlhvRTF3RHlM
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb

PLAYSTORE INFORMATION

Title: MyHealthONE

Score: 4.178827 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.hcahealthcare.mhom

Developer Details: HCA Healthcare Inc, HCA+Healthcare+Inc, None, https://myhealthone.com, support@myhealthone.com,

Release Date: Mar 25, 2020 **Privacy Policy:** Privacy link

Description:

The MyHealthONE app features are designed with you in mind: Access medical health records securely View lab results as soon as they're available Find local doctors Schedule appointments Fill out medical paperwork hassle-free Pay a bill View imaging reports Integrate with other healthcare portals Manage accounts for multiple family members Sign up for classes or events MyHealthONE simplifies the patient and caregiver experience. The easy-to-navigate healthcare mobile app lets you manage your health information and track your health journey in one convenient place. It's healthcare on your terms, when you need it. Whether you are managing your own health or that of a loved one, MyHealthONE is the partner you need in the healthcare journey. Secure and straightforward, just how healthcare should be.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:30:30	Generating Hashes	OK

2025-08-29 23:30:30	Extracting APK	OK
2025-08-29 23:30:30	Unzipping	OK
2025-08-29 23:30:30	Parsing APK with androguard	OK
2025-08-29 23:30:31	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:30:31	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:30:34	Parsing AndroidManifest.xml	OK
2025-08-29 23:30:34	Extracting Manifest Data	OK
2025-08-29 23:30:34	Manifest Analysis Started	OK
2025-08-29 23:30:34	Reading Network Security config from network_security_config.xml	OK
2025-08-29 23:30:34	Parsing Network Security config	OK
2025-08-29 23:30:34	Performing Static Analysis on: MyHealthONE (com.hcahealthcare.mhom)	OK

2025-08-29 23:30:34	Fetching Details from Play Store: com.hcahealthcare.mhom	OK
2025-08-29 23:30:35	Checking for Malware Permissions	OK
2025-08-29 23:30:35	Fetching icon path	OK
2025-08-29 23:30:35	Library Binary Analysis Started	OK
2025-08-29 23:30:35	Reading Code Signing Certificate	OK
2025-08-29 23:30:35	Running APKiD 2.1.5	OK
2025-08-29 23:30:37	Detecting Trackers	OK
2025-08-29 23:30:40	Decompiling APK to Java with JADX	OK
2025-08-29 23:30:58	Converting DEX to Smali	OK
2025-08-29 23:30:58	Code Analysis Started on - java_source	OK
2025-08-29 23:31:01	Android SBOM Analysis Completed	OK

2025-08-29 23:31:19	Android SAST Completed	OK
2025-08-29 23:31:19	Android API Analysis Started	OK
2025-08-29 23:31:33	Android API Analysis Completed	OK
2025-08-29 23:31:33	Android Permission Mapping Started	OK
2025-08-29 23:31:45	Android Permission Mapping Completed	OK
2025-08-29 23:32:05	Android Behaviour Analysis Started	OK
2025-08-29 23:32:17	Android Behaviour Analysis Completed	OK
2025-08-29 23:32:17	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:32:42	Email and URL Extraction Completed	OK
2025-08-29 23:32:42	Extracting String data from APK	OK
2025-08-29 23:32:42	Extracting String data from Code	OK

2025-08-29 23:32:42	Extracting String values and entropies from Code	OK
2025-08-29 23:32:45	Performing Malware check on extracted domains	OK
2025-08-29 23:32:50	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.