MOBSF

ANDROID STATIC ANALYSIS REPORT

LabcorpPatient (6.2.0)

File Name:	com.labcorp.patientportal_62048.apk
Package Name:	com.labcorp.patientportal
Scan Date:	Aug. 30, 2025, 11:15 p.m.
App Security Score:	81/100 (LOW RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	1	8	0

FILE INFORMATION

File Name: com.labcorp.patientportal_62048.apk
Size: 20.66MB
MD5: 767ea9c56192269c32802416e7c0d239
SHA1: 489df1f186ce1fb0672b7523aa8e36a64c32a1c3
SHA256: 8b0a64043c5cbd430afc0ba9e5699a8b27a4c19daccab4c5d2d9567bb91f1def

APP INFORMATION

App Name: LabcorpPatient
Package Name: com.labcorp.patientportal
Main Activity: com.labcorp.patientportal.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 6.2.0
Android Version Code: 62048

APP COMPONENTS

Activities: 7
Services: 0
Receivers: 1
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
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: 2018-03-13 19:45:19+00:00
Valid To: 2048-03-13 19:45:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4c89adf6d1018d081c1d6b6da67ac83d0a39ac6d
Hash Algorithm: sha256
md5: 2e8be401b7f5e079915539df242eb025
sha1: 2db59b0c7bbdb1fb9d6193219804f74612b989e2
sha256: 2831fe1b52878d43f512bb7f5052a5d2e8584f44fa133595c96e8f75000be38d
sha512: 6c7eaa063366dad9728a24d427ab9b67228c87a5173cd680019d6ab5772b172794d7dba0459c4048d4fe185bdbce2b62b23627446693041f76c3ca24e78b0a61
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 8ad2581b5eb61cde59be34f21454cbec6d2e2dcef1bcb466e541bfaac20303ca
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.labcorp.patientportal.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.labcorp.patientportal.MainActivity	Schemes: http://, https://, Hosts: patient.labcorp.com, Paths: /landing, /invoices/payment-plan-landing, Path Prefixes: /account, /portal,
io.ionic.authconnect.android.RedirectActivity	Schemes: com.labcorp.patientportal://, https://, Hosts: patient.labcorp.com, Mime Types: text/*, Path Prefixes: /mobile-callback,

NETWORK SECURITY

HIGH: 0 | WARNING: 1 | INFO: 0 | SECURE: 7

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	labcorp.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
4	labcorp.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: xv58t0BM8ZKgRjjOFuCcQaIX4wVuogBK+wBfyxARBoM= Digest: SHA-256,Pin: BkLBZ52R1rQb3aXioxU+yoNnYygXhKZ64kLAGhKqWQA= Digest: SHA-256,Pin: K07auRvrqCRqo7VK4kF0c0Yut2KQxHSIL1LRuJKLvhQ= Digest: SHA-256,Pin: uxBufth1aionUOCs6NXgxIKzuSX85W7xOMlSF5dJNqc= Digest: SHA-256,Pin: DxH4tt40L+eduF6szpY6TONlxhZhBd+pJ9wbHlQ2fuw= Digest: SHA-256,Pin: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= Digest: SHA-256,Pin: +80xuW/iJNoYOv/l7WXhpeNFPD6l/xY0aBAP9d+F4fM= Digest: SHA-256,Pin: Wec45nQiFwKvHtuHxSAMGkt19k+uPSw9JlEkxhvYPHk= Digest: SHA-256,Pin: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= Digest: SHA-256,Pin: is6+4lKts9NjVnU4SWeJI5haSDctPy0Y7Bl3wP8zqdY= Digest: SHA-256,Pin: R3hcMOAGw0WFztuG2skTodoHp8IGid3Qg63Cn7YUYoM= Digest: SHA-256,Pin: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Digest: SHA-256,Pin: 4FS+KCAlsoL9ph71nS8miEvq9iVIY6Ii7fkMZNCR1tk= Digest: SHA-256,Pin: Wec45nQiFwKvHtuHxSAMGkt19k+uPSw9JlEkxhvYPHk= Digest: SHA-256,Pin: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= Digest: SHA-256,Pin: kk/IIMNCNpNU+MA1J1lwtrqgDHmIJ/+pmMAKN7jmCPg= Digest: SHA-256,Pin: RRM1dGqnDFsCJXBTHky16vi1obOlCgFFn/yOhI/y+ho= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256]
5	data.patient.pendo.cws.labcorp.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: WYj6yWCAtpBuBg7cn0Xrn7B3zzmhlPXQnTBGq2VIFAo= Digest: SHA-256,Pin: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc= Digest: SHA-256]

NO	SCOPE	SEVERITY	DESCRIPTION
6	login-patientdev.sb.cws.labcorp.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: HWZqI0GohylH0b/dYW1GYusZX8O62ATsJmP0+AdWWpA= Digest: SHA-256,Pin: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= Digest: SHA-256]
7	js.braintreegateway.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: HXweMh+KfuJWS5NRMaU7PFrwQDL5jrVS+5NyQG/y5LE= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256]
8	content.patient.pendo.cws.labcorp.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: p+DncO6UB3Ew0/ZMDnFKbdUEkHTfWloLKhbhDXons5E= Digest: SHA-256,Pin: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= 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: **1** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. 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.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (io.ionic.authconnect.android.RedirectActivity) 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.
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: **3** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bottlerocketstudios/vault/StandardSharedPreferenceVault.java com/bottlerocketstudios/vault/keys/generator/PbkdfKeyGenerator.java com/bottlerocketstudios/vault/keys/storage/CompatSharedPrefKeyStorageFactory.java com/bottlerocketstudios/vault/keys/storage/KeychainAuthenticatedKeyStorage.java com/bottlerocketstudios/vault/keys/storage/SharedPrefKeyStorage.java com/bottlerocketstudios/vault/keys/storage/hardware/AndroidKeystoreTester.java com/bottlerocketstudios/vault/keys/wrapper/ObfuscatingSecretKeyWrapper.java com/bottlerocketstudios/vault/salt/SaltBox.java com/getcapacitor/Logger.java com/ionicframework/IdentityVault/BiometricPromptActivity.java com/ionicframework/IdentityVault/Device.java com/ionicframework/IdentityVault/DeviceSecurityFactory.java com/ionicframework/IdentityVault/DeviceSecurityStrongVault.java com/ionicframework/IdentityVault/IdentityVaultPlugin.java com/ionicframework/IdentityVault/NonVaultBiometricPromptActivity.java com/ionicframework/IdentityVault/VaultPlugin.java com/ionicframework/auth/IdentityVault.java com/ionicframework/auth/IonicCombinedVault.java com/ionicframework/auth/IonicKeychainAuthenticatedStorage.java com/ionicframework/auth/IonicSharedPreferenceVault.java io/capawesome/capacitorjs/plugins/fileopener/FileOpenerPlugin.java io/ionic/authconnect/android/AuthActivityManager.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a io/ionic/authconnect/android/Logger.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/ionicframework/IdentityVault/DevicePlugin.java com/ionicframework/auth/IonicCombinedVault.java com/ionicframework/auth/IonicSharedPreferenceVault.java com/ionicframework/auth/VaultFactory.java com/ionicframework/auth/VaultState.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/BridgeWebChromeClient.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/ionic/authconnect/android/AuthConnect$fetchToken$1.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/ionic/authconnect/android/AuthConnect$fetchToken$1.java
00089	Connect to a URL and receive input stream from the server	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/ionic/authconnect/android/AuthConnect$fetchToken$1.java
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/ionic/authconnect/android/AuthConnect$fetchToken$1.java
00109	Connect to a URL and get the response code	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java io/ionic/authconnect/android/AuthConnect$fetchToken$1.java
00094	Connect to a URL and read data from it	command network	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/capacitorjs/plugins/filesystem/Filesystem.java com/capacitorjs/plugins/filesystem/FilesystemPlugin.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00036	Get resource file from res/raw directory	reflection	com/capacitorjs/plugins/browser/Browser.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/capacitorjs/plugins/browser/BrowserPlugin.java com/getcapacitor/Bridge.java io/capawesome/capacitorjs/plugins/fileopener/FileOpener.java io/ionic/authconnect/android/AuthActivityManager.java io/ionic/authconnect/android/AuthConnect.java
00091	Retrieve data from broadcast	collection	com/getcapacitor/Bridge.java com/ionicframework/auth/IonicNativeAuth.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java
00013	Read file and put it into a stream	file	com/capacitorjs/plugins/filesystem/Filesystem.java com/getcapacitor/AndroidProtocolHandler.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/filesystem/Filesystem.java
00192	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	0/44	

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
google.com	ok	**IP:** 142.250.176.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ionic.io	ok	**IP:** 104.20.24.198 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
capacitorjs.com	ok	**IP:** 172.67.203.214 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
1eRHtJaybutdAsFp2DkfrT1FqMJlLfT7DdgCpQtTaoQWheoeFBZRqt5pgFDH7Cf

PLAYSTORE INFORMATION

Title: Labcorp | Patient

Score: 3.8888888 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.labcorp.patientportal

Developer Details: Labcorp, Labcorp, None, https://www.labcorp.com, PatientMobileSupport@labcorp.com,

Release Date: Apr 19, 2018 **Privacy Policy:** Privacy link

Description:

The Labcorp Patient mobile app is easy to use and has convenient features that help you manage your health. Here are just a few of the things you can do, from the convenience of your mobile device: • Find a lab and schedule an appointment • Check in at a Patient Service Center by scanning a QR code at our kiosk or checking in from your mobile device • Receive a notification when your lab test results are ready • View, download, and print your official lab test result report • View historical lab test results • Receive a notification when a bill is available • View, download, print, and pay your bills • Share your account with someone else • Add minors to your account to manage their lab testing information • Manage your profile preferences • Reset your password • Log in using your Face ID or Fingerprint • Learn how you can participate in clinical research offered by Labcorp

SCAN LOGS

Timestamp	Event	Error
2025-08-30 23:15:58	Generating Hashes	OK
2025-08-30 23:15:58	Extracting APK	OK
2025-08-30 23:15:58	Unzipping	OK

2025-08-30 23:15:58	Parsing APK with androguard	OK
2025-08-30 23:15:58	Extracting APK features using aapt/aapt2	OK
2025-08-30 23:15:59	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 23:16:01	Parsing AndroidManifest.xml	OK
2025-08-30 23:16:01	Extracting Manifest Data	OK
2025-08-30 23:16:01	Manifest Analysis Started	OK
2025-08-30 23:16:01	Reading Network Security config from network_security_config.xml	OK
2025-08-30 23:16:01	Parsing Network Security config	OK
2025-08-30 23:16:01	Performing Static Analysis on: LabcorpPatient (com.labcorp.patientportal)	OK
2025-08-30 23:16:02	Fetching Details from Play Store: com.labcorp.patientportal	OK
2025-08-30 23:16:02	Checking for Malware Permissions	OK

2025-08-30 23:16:02	Fetching icon path	OK
2025-08-30 23:16:02	Library Binary Analysis Started	OK
2025-08-30 23:16:02	Reading Code Signing Certificate	OK
2025-08-30 23:16:03	Running APKiD 2.1.5	OK
2025-08-30 23:16:08	Detecting Trackers	OK
2025-08-30 23:16:09	Decompiling APK to Java with JADX	OK
2025-08-30 23:16:20	Converting DEX to Smali	OK
2025-08-30 23:16:20	Code Analysis Started on - java_source	OK
2025-08-30 23:16:21	Android SBOM Analysis Completed	OK
2025-08-30 23:16:27	Android SAST Completed	OK

2025-08-30 23:16:27	Android API Analysis Started	OK
2025-08-30 23:16:32	Android API Analysis Completed	OK
2025-08-30 23:16:32	Android Permission Mapping Started	OK
2025-08-30 23:16:37	Android Permission Mapping Completed	OK
2025-08-30 23:16:38	Android Behaviour Analysis Started	OK
2025-08-30 23:16:43	Android Behaviour Analysis Completed	OK
2025-08-30 23:16:43	Extracting Emails and URLs from Source Code	OK
2025-08-30 23:16:43	Email and URL Extraction Completed	OK
2025-08-30 23:16:43	Extracting String data from APK	OK
2025-08-30 23:16:43	Extracting String data from Code	OK

2025-08-30 23:16:43	Extracting String values and entropies from Code	OK
2025-08-30 23:16:44	Performing Malware check on extracted domains	OK
2025-08-30 23:16:47	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.