ANDROID STATIC ANALYSIS REPORT

IHSS EVV Mobile App (1.2.0)

File Name:	gov.ca.ihss.evv_102000.apk
Package Name:	gov.ca.ihss.evv
Scan Date:	Sept. 1, 2025, 1:22 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	9	2	2	1

FILE INFORMATION

File Name: gov.ca.ihss.evv_102000.apk
Size: 22.35MB
MD5: f505034faa17e122856d45f81ed1b027
SHA1: e0c3be691f745fc042d5b449ea97a10acbd5ea54
SHA256: 22413209e7c78211c1a0e211f359273c67d05154404c284f88c42ea10142730f

APP INFORMATION

App Name: IHSS EVV Mobile App
Package Name: gov.ca.ihss.evv
Main Activity: gov.ca.ihss.evv.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 1.2.0
Android Version Code: 102000

APP COMPONENTS

Activities: 5
Services: 0
Receivers: 1
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
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: 2021-04-21 16:08:26+00:00
Valid To: 2051-04-21 16:08:26+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xad71b0e330a793780cd9eb0359144e14b907d798
Hash Algorithm: sha256
md5: d93c194afbac3db4a6f0199227e49b28
sha1: 87bdb8fda519f685b1b5764215571eda99d8c8a6
sha256: da635ab801c713ef0731d39753d7cab2e255ff16891a2609d9aee5d191f352c0
sha512: 050270eb77e488ab52dda043c77eb7684ca14cbc4162fa83c6baa338165babd769dacc090b63e253f2a7789fa4171924c93b4fffdf2a58c410264d87f5153a2a
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 838a375dda239338108707fcf311fcbd19066481d5ed5241da2d4f04af774286
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.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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
gov.ca.ihss.evv.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>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
Build.TAGS check
possible ro.secure 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>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></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: **0**

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **2** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	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: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bottlerocketstudios/vault/StandardSharedPreferenceVault.java com/bottlerocketstudios/vault/keys/generator/PbkdfKeyGenerator.java com/bottlerocketstudios/vault/keys/storage/CompatSharedPrefKeyStorageFactory.java com/bottlerocketstudios/vault/keys/storag

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	e/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/capacitorjs/plugins/network/NetworkPlugin.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 com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java com/xmartlabs/cordova/market/Market.java cordova/plugin/RequestLocationAccuracy.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLitePlugin.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/Const.java de/cyberkatze/iroot/Constants.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/RootBeer.java de/cyberkatze/iroot/Constants.java de/cyberkatze/iroot/InternalRootDetection.java
5	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/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.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	com/getcapacitor/BridgeWebChromeClient.java
7	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	io/sqlc/SQLiteAndroidDatabase.java net/sqlcipher/database/SupportHelper.java
8	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	net/sqlcipher/database/SQLiteDatabase.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00022	Open a file from given absolute path of the file	file	com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java io/sqlc/SQLitePlugin.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/FileUtils.java
00096	Connect to a URL and set request method	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.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
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
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

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00094	Connect to a URL and read data from it	command network	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
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/getcapacitor/Bridge.java com/phonegap/plugins/nativesettings/NativeSettings.java com/xmartlabs/cordova/market/Market.java
00091	Retrieve data from broadcast	collection	com/getcapacitor/Bridge.java com/ionicframework/auth/IonicNativeAuth.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java
00036	Get resource file from res/raw directory	reflection	com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java com/phonegap/plugins/nativesettings/NativeSettings.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorHttpUrlConnection.java
00075	Get location of the device	collection location	com/capacitorjs/plugins/geolocation/Geolocation.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java
00005	Get absolute path of file and put it to JSON object	file	io/sqlc/SQLitePlugin.java
00013	Read file and put it into a stream	file	com/getcapacitor/AndroidProtocolHandler.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, 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
www.zetetic.net	ok	**IP:** 18.238.96.30 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ionic.io	ok	**IP:** 172.66.164.120 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
1eRHtJaybutdAsFp2DkfrT1FqMJlLfT7DdgCpQtTaoQWheoeFBZRqt5pgFDH7Cf

PLAYSTORE INFORMATION

Title: IHSS EVV Mobile App

Score: 4.47 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** gov.ca.ihss.evv

Developer Details: CalHHS OTSI, CalHHS+OTSI, None, https://www.cdss.ca.gov/in-home-supportive-services, cmipsmobilesupport@osi.ca.gov,

Release Date: Feb 21, 2022 **Privacy Policy:** Privacy link

Description:

California’s In-Home Supportive Services (IHSS) Program, Electronic Visit Verification (EVV) Solution for IHSS & WPCS Providers. IHSS & WPCS providers will check-in at the beginning and check-out at the end of each work day for each IHSS/WPCS recipient they provide services for with simple easy to use screens. Providers are guided step-by-step to choose the recipient they are working for, if they would like to check-in or check-out, and select if they are in the home or in the community. Additionally, the app will conveniently add the provider’s hours to their IHSS Timesheet at the end of their workday. While the IHSS EVV app captures the start time, end time, and location of the visit using Location Services, it does not track the provider during the visit or at any other time. It simply takes a snapshot of the location when they check-in at the beginning and check-out at the end of each work day. California’s IHSS EVV Solution is in full compliance with the 21st Century Cures Act Federal EVV requirements by capturing: - The date, time, and location where the IHSS/WPCS services start, - The name of the recipient, - The date, time, and location where the IHSS/WPCS services end, and - The location the visit ends. California’s IHSS EVV Solution also allows for complete capturing of data when the user does not have internet connectivity. The IHSS EVV app will store the encrypted visit information and will transmit the data once the user has internet connectivity.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:22:13	Generating Hashes	OK
2025-09-01 13:22:13	Extracting APK	OK
2025-09-01 13:22:13	Unzipping	OK
2025-09-01 13:22:23	Parsing APK with androguard	OK
2025-09-01 13:22:23	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:22:23	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:22:26	Parsing AndroidManifest.xml	OK
2025-09-01 13:22:26	Extracting Manifest Data	OK
2025-09-01 13:22:26	Manifest Analysis Started	OK
2025-09-01 13:22:26	Reading Network Security config from network_security_config.xml	OK

2025-09-01 13:22:26	Parsing Network Security config	OK
2025-09-01 13:22:26	Performing Static Analysis on: IHSS EVV Mobile App (gov.ca.ihss.evv)	OK
2025-09-01 13:22:28	Fetching Details from Play Store: gov.ca.ihss.evv	OK
2025-09-01 13:22:29	Checking for Malware Permissions	OK
2025-09-01 13:22:29	Fetching icon path	OK
2025-09-01 13:22:29	Library Binary Analysis Started	OK
2025-09-01 13:22:30	Reading Code Signing Certificate	OK
2025-09-01 13:22:31	Running APKiD 2.1.5	OK
2025-09-01 13:22:34	Detecting Trackers	OK
2025-09-01 13:22:35	Decompiling APK to Java with JADX	OK

2025-09-01 13:22:44	Converting DEX to Smali	OK
2025-09-01 13:22:44	Code Analysis Started on - java_source	OK
2025-09-01 13:22:53	Android SBOM Analysis Completed	OK
2025-09-01 13:22:56	Android SAST Completed	OK
2025-09-01 13:22:56	Android API Analysis Started	OK
2025-09-01 13:23:08	Android API Analysis Completed	OK
2025-09-01 13:23:08	Android Permission Mapping Started	OK
2025-09-01 13:23:17	Android Permission Mapping Completed	OK
2025-09-01 13:23:17	Android Behaviour Analysis Started	OK
2025-09-01 13:23:19	Android Behaviour Analysis Completed	OK

2025-09-01 13:23:19	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:23:19	Email and URL Extraction Completed	OK
2025-09-01 13:23:19	Extracting String data from APK	OK
2025-09-01 13:23:19	Extracting String data from Code	OK
2025-09-01 13:23:19	Extracting String values and entropies from Code	OK
2025-09-01 13:23:22	Performing Malware check on extracted domains	OK
2025-09-01 13:23:28	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.