MOBSF

ANDROID STATIC ANALYSIS REPORT

Dexcom G6 (1.14.0.0)

File Name:	com.dexcom.g6_1140000.apk
Package Name:	com.dexcom.g6
Scan Date:	Aug. 29, 2025, 9:39 p.m.

App Security Score: 60/100 (LOW RISK)

Grade: A

Trackers Detection: 4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	12	3	3	1

FILE INFORMATION

File Name: com.dexcom.g6_1140000.apk
Size: 61.19MB
MD5: 8b5c8b3a41a84e395258f017414dde1b
SHA1: eb16e6263e91ac7dfde1da271601863a58c1e94d
SHA256: 5c2c3b49ff728b8c14903ffb499476599fec7c5d8e5e5860f4106be37d58826c

APP INFORMATION

App Name: Dexcom G6
Package Name: com.dexcom.g6
Main Activity: com.dexcom.cgm.activities.AppCompatabilityActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.14.0.0
Android Version Code: 1140000

APP COMPONENTS

Activities: 84
Services: 14
Receivers: 9
Providers: 4
Exported Activities: 4
Exported Services: 2
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=CA, L=San Diego, O=Dexcom, OU=Research and Development, CN=Android Development Team
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-09-25 15:38:39+00:00
Valid To: 2040-09-18 15:38:39+00:00
Issuer: C=US, ST=CA, L=San Diego, O=Dexcom, OU=Research and Development, CN=Android Development Team
Serial Number: 0x1a7999a7
Hash Algorithm: sha256
md5: f81482a82de6c68428c0cd55f91b72f5
sha1: 050f7b7bdc16dd198c2770d69182ceddbc443184

sha256: 2c5aa799006136a39e7ca2d6d3460856e51470e52ea21c0535ab0c127f2a4da6
sha512: a3a1b5b67eb969a172849ca348c67fb1500e4c1332ab75ae6d85e763354f1329f7eb2be9bb1bc275bdf66feb2639f0520fc7062bec876785f19ff467962d9734
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3b599f658e7b26142073b3521f46e84157de2a478494ce8939d050dccd181836
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
com.google.android.permission.PROVIDE_BACKGROUND	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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_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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
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.
android.permission.health.WRITE_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.dexcom.g6.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>8b5c8b3a41a84e395258f017414dde1b.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>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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>SIM operator check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>res/sq.apk!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>Compiler</td><td>r8 without marker (suspicious)</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>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes.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>Anti-VM Code</td><td>Build.MODEL check Build.PRODUCT check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.dexcom.cgm.activities.AppCompatabilityActivity	Schemes: dexcomg6://,

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: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config_release]	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.dexcom.cgm.activities.HealthConnectActivity) 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.
3	Activity-Alias (com.dexcom.cgm.activities.AndroidUHealthConnectActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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	Activity (com.dexcom.cgm.activities.NotificationTrampolineActivity) 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	Activity (com.dexcom.cgm.activities.MenuActivity) 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.
6	Content Provider (com.dexcom.g6.content_provider.CgmContentProvider) is Protected by a permission. Permission: com.dexcom.g6.content_provider.READ_PERMISSION protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
7	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [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.
8	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.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **2** | SECURE: **1** | 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/dexcom/cgm/activities/AndroidDatabaseLogProxy.java com/dexcom/cgm/activities/AndroidLogProxy.java com/dexcom/platform_database/database/tables/BaseTable.java kt/AbstractC4447.java kt/C1300.java kt/C2511.java kt/C3805.java kt/C4000.java kt/C4701.java kt/C4760.java kt/ServiceConnectionC0079.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteQueryBuilder.java org/joda/time/tz/ZoneInfoCompiler.java retrofit/Platform.java
2	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/dexcom/cgm/CgmApplication.java com/dexcom/cgm/activities/setupwizard/WelcomeScreen.java com/dexcom/platform_database/database/CgmDatabaseComponent.java kt/C4277.java kt/C4884.java
3	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/dexcom/cgm/CgmApplication.java com/dexcom/cgm/activities/WebLoginActivity.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	com/qualtrics/digital/SamplingUtil.java kt/AbstractC3542.java kt/AbstractC3956.java kt/C0327.java kt/C1490.java kt/C3150.java kt/C4018.java kt/C4382.java kt/C4414.java kt/C4532.java kt/C4996.java
5	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	kt/C1027.java kt/C2282.java kt/C2387.java kt/C3662.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	kt/C0093.java kt/C1793.java kt/C4770.java kt/C4974.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/dexcom/platform_database/database/CgmDatabaseComponent.java
8	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/dexcom/cgm/activities/setupwizard/LegalAgreementsActivity.java com/qualtrics/digital/QualtricsSurveyFragment.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
2	arm64-v8a/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
4	x86_64/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.
5	armeabi-v7a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.
7	armeabi/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
8	x86/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.
10	arm64-v8a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
11	arm64-v8a/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
13	x86_64/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.
14	armeabi-v7a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.
16	armeabi/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
17	x86/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86/libxrfrakhi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/dexcom/cgm/CgmApplication.java com/dexcom/cgm/test/api/SetupConfiguration.java kt/C0123.java kt/C0338.java kt/C1027.java kt/C2282.java kt/C2387.java kt/C3492.java kt/C4277.java retrofit/mime/TypedFile.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/dexcom/cgm/activities/AppCompatabilityActivity.java com/dexcom/cgm/activities/BatteryOptimizingActivity.java com/dexcom/cgm/activities/CGMStateFragment.java com/dexcom/cgm/activities/DexWebViewActivity.java com/dexcom/cgm/activities/EnableNotificationsActivity.java com/dexcom/cgm/activities/HealthConnectActivity.java com/dexcom/cgm/activities/TrendGraphFragment.java com/dexcom/cgm/activities/VideoViewActivity.java com/dexcom/cgm/activities/WebLoginActivity.java com/dexcom/cgm/activities/event_entry/EventHistoryActivity.java com/dexcom/cgm/activities/setupwizard/SetupWizardActivity.java com/dexcom/cgm/activities/share/RemoteMonitoringTutorialActivity.java com/dexcom/cgm/activities/share/ShareMainActivity.java com/dexcom/cgm/activities/support/ContactDexcomActivity.java com/dexcom/cgm/activities/support/SupportBaseActivity.java com/dexcom/cgm/activities/support/TechSupportHelper.java com/qualtrics/digital/QualtricsNotificationManager.java com/qualtrics/digital/QualtricsPopOverActivity.java kt/C0426.java kt/C1307.java kt/C5005.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	kt/C0695.java kt/C1223.java
00013	Read file and put it into a stream	file	com/dexcom/cgm/test/api/SetupConfiguration.java kt/C0865.java kt/C2282.java kt/C2381.java kt/C3797.java kt/C4195.java kt/C4277.java kt/C4563.java kt/C4632.java kt/C4884.java kt/C5005.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java retrofit/mime/TypedFile.java
00137	Get last known location of the device	location collection	kt/C1690.java
00125	Check if the given file path exist	file	kt/C0106.java kt/C4632.java
00162	Create InetSocketAddress object and connecting to it	socket	kt/C0093.java kt/C2409.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	kt/C0093.java kt/C2409.java
00091	Retrieve data from broadcast	collection	com/dexcom/cgm/activities/DexWebViewActivity.java com/dexcom/cgm/activities/MenuActivity.java com/dexcom/cgm/activities/MeterEntryActivity.java com/flurry/android/FlurryInstallReceiver.java com/qualtrics/digital/QualtricsNotificationManager.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/dexcom/cgm/activities/BatteryOptimizingActivity.java com/dexcom/cgm/activities/DexWebViewActivity.java com/dexcom/cgm/activities/EnableNotificationsActivity.java com/dexcom/cgm/activities/HealthConnectActivity.java com/dexcom/cgm/activities/TrendGraphFragment.java com/dexcom/cgm/activities/event_entry/EventHistoryActivity.java com/dexcom/cgm/activities/setupwizard/SetupWizardActivity.java com/dexcom/cgm/activities/share/RemoteMonitoringTutorialActivity.java com/dexcom/cgm/activities/share/ShareMainActivity.java com/dexcom/cgm/activities/support/TechSupportHelper.java com/qualtrics/digital/QualtricsNotificationManager.java
00078	Get the network operator name	collection telephony	kt/C4342.java
00160	Use accessibility service to perform action getting node info by View Id	accessibility service	kt/C1223.java
00161	Perform accessibility service action on accessibility node info	accessibility service	kt/C1223.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	kt/C1223.java
00175	Get notification manager and cancel notifications	notification	kt/C0569.java
00036	Get resource file from res/raw directory	reflection	com/dexcom/cgm/activities/BatteryOptimizingActivity.java com/dexcom/cgm/activities/setupwizard/SetupWizardActivity.java com/dexcom/cgm/activities/share/RemoteMonitoringTutorialActivity.java kt/C1307.java kt/C5005.java kt/ViewOnClickListenerC3734.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	kt/C5005.java
00112	Get the date of the calendar event	collection calendar	kt/C3176.java org/joda/time/LocalDateTime.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	kt/C2951.java
00056	Modify voice volume	control	com/dexcom/cgm/activities/notifications/VolumeManipulator.java
00015	Put buffer stream (data) to JSON object	file	kt/C1567.java
00096	Connect to a URL and set request method	command network	kt/C1567.java retrofit/client/UrlConnectionClient.java
00089	Connect to a URL and receive input stream from the server	command network	kt/C1567.java retrofit/client/UrlConnectionClient.java
00109	Connect to a URL and get the response code	network command	kt/C1567.java retrofit/client/UrlConnectionClient.java
00094	Connect to a URL and read data from it	command network	kt/C1567.java
00108	Read the input stream from given URL	network command	kt/C1567.java
00147	Get the time of current location	collection location	kt/C4471.java
00075	Get location of the device	collection location	kt/C4471.java
00115	Get last known location of the device	collection location	kt/C4471.java
00121	Create a directory	file command	kt/C0106.java
00033	Query the IMEI number	collection	kt/C3797.java
00191	Get messages in the SMS inbox	sms	kt/ViewOnClickListenerC3734.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://g6-store-us.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/239952856118/namespaces/firebase:fetch?key=AIzaSyDroULjdU0FK2kW5DaNk_r5CBP5UU-Cvss. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	8/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, 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
android.googlesource.com	ok	**IP:** 142.251.15.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.dexcom.com	ok	**IP:** 162.159.130.80 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
g6-store-us.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

EMAILS

EMAIL	FILE
a5@j.b6	kt/EnumC4899.java
a@j.zpn	kt/C0292.java
a@4.66	kt/C3662.java
y@9k.np	kt/ViewOnClickListenerC3734.java
zii39tbj@z2x.lsbl	kt/C4853.java
u0004@c.15	kt/C2122.java
u00100@a7eip578.74b	com/dexcom/cgm/activities/setupwizard/SetupWizardActivity.java

EMAIL	FILE
m@rq.jr	lib/arm64-v8a/libxrfrakhi.so
m@rq.jr	apktool_out/lib/arm64-v8a/libxrfrakhi.so

TRACKERS

TRACKER	CATEGORIES	URL
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyDroULjdU0FK2kW5DaNk_r5CBP5UU-Cvss"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyDroULjdU0FK2kW5DaNk_r5CBP5UU-Cvss"
"firebase_database_url" : "https://g6-store-us.firebaseio.com"
"account_edit_username" : "Username"

PLAYSTORE INFORMATION

Title: Dexcom G6

Score: 3.0752532 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.dexcom.g6

Developer Details: Dexcom, Dexcom, None, http://www.dexcom.com/support, appsupport@dexcom.com,

Release Date: Apr 25, 2018 **Privacy Policy:** Privacy link

Description:

Only use this app if you have the Dexcom G6 or G6 Pro CGM Systems. Always know your glucose number and where it's heading with the Dexcom G6 and G6 Pro Continuous Glucose Monitoring (CGM) Systems –indicated for diabetes treatment decisions with zero fingersticks and no calibration.* A core feature of the Dexcom G6 and G6 Pro Systems is providing users with alarm/alerts based on their glucose level. *Fingersticks required for diabetes management decisions if symptoms do not match readings. Dexcom G6 and G6 Pro provide real-time glucose readings for patients with type 1 or type 2 diabetes every five minutes. Dexcom G6 and G6 Pro are indicated for children age 2 years and older. The Dexcom G6 and G6 Pro Systems provide personalized trend alerts right on your smart device and lets you see when your glucose levels are going too low, or too high, so you can better manage your diabetes. The Alert Schedule** feature lets you schedule and customize a second set of alerts. For example, you can set the schedule to match your work hours and have different alert settings during the rest of the day. Custom alert sounds are available, including a Vibrate-Only option on the phone for glucose alerts. The only exception is the Urgent Low Alarm, which you can't turn off. The Always Sound** setting, which is on by default, allows you to receive certain Dexcom CGM Alerts even if your phone sound is off, set to vibrate, or in Do Not Disturb mode. This will allow you to silence calls or texts but still receive audible CGM Alarm and Alerts, including the Urgent Low Alarm, Low and High Glucose alerts, Urgent Low Soon Alert**, and Rise and Fall Rate alerts**. A Home screen icon shows you if your Alerts will sound or not. For safety, the Urgent Low Alarm and three alerts cannot be silenced: Transmitter Failed, Sensor Failed, and App Stopped. Other features: Share** your glucose data with up to ten followers in real time. Followers can monitor your glucose data and trends in real time on their compatible smart device with the Dexcom Follow** app. Share and Follow functions require an internet connection. Health Connect access so you can share retrospective glucose data with third party apps Quick Glance allows you to view your glucose data on the lock screen of your smart device **Not available on Dexcom G6 Pro System Wear OS Integration allows you to view glucose alerts and alarms from your Wear OS watch.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:39:02	Generating Hashes	OK
2025-08-29 21:39:02	Extracting APK	OK
2025-08-29 21:39:02	Unzipping	OK
2025-08-29 21:39:02	Parsing APK with androguard	OK
2025-08-29 21:39:02	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:39:03	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:39:05	Parsing AndroidManifest.xml	OK
2025-08-29 21:39:05	Extracting Manifest Data	OK
2025-08-29 21:39:05	Manifest Analysis Started	OK

2025-08-29 21:39:05	Reading Network Security config from network_security_config_release.xml	OK
2025-08-29 21:39:05	Parsing Network Security config	OK
2025-08-29 21:39:05	Performing Static Analysis on: Dexcom G6 (com.dexcom.g6)	OK
2025-08-29 21:39:06	Fetching Details from Play Store: com.dexcom.g6	OK
2025-08-29 21:39:06	Checking for Malware Permissions	OK
2025-08-29 21:39:06	Fetching icon path	OK
2025-08-29 21:39:06	Library Binary Analysis Started	OK
2025-08-29 21:39:06	Analyzing lib/arm64-v8a/libsqlcipher.so	OK
2025-08-29 21:39:06	Analyzing lib/arm64-v8a/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing lib/x86_64/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing lib/x86_64/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing lib/armeabi-v7a/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing lib/armeabi-v7a/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing lib/armeabi/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing lib/x86/libsqlcipher.so	OK

2025-08-29 21:39:07	Analyzing lib/x86/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/arm64-v8a/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/arm64-v8a/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/x86_64/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/x86_64/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/armeabi-v7a/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/armeabi-v7a/libxrfrakhi.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/armeabi/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/x86/libsqlcipher.so	OK
2025-08-29 21:39:07	Analyzing apktool_out/lib/x86/libxrfrakhi.so	OK
2025-08-29 21:39:07	Reading Code Signing Certificate	OK
2025-08-29 21:39:08	Running APKiD 2.1.5	OK
2025-08-29 21:39:12	Detecting Trackers	OK
2025-08-29 21:39:14	Decompiling APK to Java with JADX	OK
2025-08-29 21:39:42	Converting DEX to Smali	OK

2025-08-29 21:39:42	Code Analysis Started on - java_source	OK
2025-08-29 21:39:47	Android SBOM Analysis Completed	OK
2025-08-29 21:40:11	Android SAST Completed	OK
2025-08-29 21:40:11	Android API Analysis Started	OK
2025-08-29 21:40:29	Android API Analysis Completed	OK
2025-08-29 21:40:29	Android Permission Mapping Started	OK
2025-08-29 21:40:49	Android Permission Mapping Completed	OK
2025-08-29 21:40:50	Android Behaviour Analysis Started	OK
2025-08-29 21:41:09	Android Behaviour Analysis Completed	OK
2025-08-29 21:41:09	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:41:17	Email and URL Extraction Completed	OK
2025-08-29 21:41:17	Extracting String data from APK	OK
2025-08-29 21:41:17	Extracting String data from SO	OK
2025-08-29 21:41:17	Extracting String data from Code	OK
2025-08-29 21:41:17	Extracting String values and entropies from Code	OK

2025-08-29 21:41:22	Performing Malware check on extracted domains	OK
2025-08-29 21:41:24	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.