MOBSF

ANDROID STATIC ANALYSIS REPORT

ODK Collect (v2022.2.3)

File Name:	ODK-Collect-v2022.2.3.apk
Package Name:	org.odk.collect.android
Scan Date:	July 5, 2022, 9:24 a.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	24	3	1	2

FILE INFORMATION

File Name: ODK-Collect-v2022.2.3.apk
Size: 12.87MB
MD5: 2eb5650565feb0f9291d4ba934af6ff2
SHA1: be2f28c3e75874981e41d3b3485c7e8d96792ea6
SHA256: fff9a07d1ae75110f9ecc0717b12fa0286fb2faf5349d6b788e7222d20999af3

APP INFORMATION

App Name: ODK Collect
Package Name: org.odk.collect.android
Main Activity:
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: v2022.2.3

Android Version Code: 4444

APP COMPONENTS

Activities: 35
Services: 14
Receivers: 10
Providers: 6
Exported Activities: 9
Exported Services: 2
Exported Receivers: 1
Exported Providers: 2

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=ODK Team
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-10-17 21:11:38+00:00
Valid To: 2034-10-11 21:11:38+00:00
Issuer: CN=ODK Team
Serial Number: 0x4ada330a
Hash Algorithm: sha1
md5: c337063518f22ab426d8e3e17dc22d08
sha1: a18c96798438ad8479a687373c8966459b7d4300
sha256: dcd4b94b1e0c3d9669223d45cdc0e2f0cc6ded12a7e6efab49ba36b3d1d48dd8
sha512: 3135444501e40e7c29404706e291f2f24e9b4dfb737be790fc04e613ae3a8fca985b24d41d69034ea655296d02c81eab337beda72c6e303ce4476cb678f4b8cd
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 8e78232959ad3d0aae57a04183b2952a43c541c53475678ec2ed0eaa9fe8f2c9

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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.

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.HARDWARE check
Build.TAGS check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</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>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>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	info	Base config is configured to trustbundled certs @raw/isrgrootx1.
3	*	warning	Base config is configured to trust system certificates.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity-Alias (org.odk.collect.android.activities.FormEntryActivity) is not Protected. [android:exported=true]	high	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.
5	Activity-Alias (org.odk.collect.android.activities.InstanceChooserList) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
6	Activity-Alias (org.odk.collect.android.activities.FormChooserList) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
7	Activity-Alias (org.odk.collect.android.activities.FormDownloadList) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
8	Activity-Alias (org.odk.collect.android.activities.InstanceUploaderList) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
9	Activity-Alias (org.odk.collect.android.activities.InstanceUploaderActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Activity-Alias (org.odk.collect.android.activities.SplashScreenActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
11	Content Provider (org.odk.collect.android.external.FormsProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Content Provider (org.odk.collect.android.external.InstanceProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (org.odk.collect.android.external.AndroidShortcutsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
14	Activity (org.odk.collect.android.external.FormUriActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	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.
17	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mapbox/android/telemetry/location/LocationEngineControllerImpl.java com/caverock/androidsvg/CSSParser.java com/mapbox/android/telemetry/provider/MapboxTelemetryInitProvider.java com/bumptech/glide/util/pool/FactoryPools.java com/mapbox/android/core/crashreporter/CrashReportBuilder.java com/mapbox/android/gestures/MultiFingerGesture.java org/slf4j/helpers/Util.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/load/engine/Engine.java org/osmdroid/tileprovider/util/CloudmadeUtil.java org/osmdroid/tileprovider/modules/ArchiveFileFactory.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java org/osmdroid/views/MapView.java org/osmdroid/tileprovider/modules/TileDownloader.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/mapbox/android/telemetry/ComServerInformation.java org/osmdroid/tileprovider/modules/MapTileModuleProviderBase.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/request/target/ViewTa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/request/target/ViewTarget.java org/osmdroid/tileprovider/modules/MapTileDownloader.java com/mapbox/android/telemetry/MapboxTelemetry.java com/bumptech/glide/Glide.java org/osmdroid/views/overlay/TilesOverlay.java com/mapbox/android/telemetry/errors/ErrorReporterEngine.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/engine/executor/GlideExecutor.java org/osmdroid/tileprovider/modules/TileWriter.java com/mapbox/android/telemetry/errors/ErrorUtils.java com/caverock/androidsvg/SVGAndroidRenderer.java com/mapbox/android/core/crashreporter/MapboxUncaughtExceptionHanlder.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/journeyapps/barcodescanner/DecoderThread.java org/osmdroid/tileprovider/MapTileProviderBase.java com/bumptech/glide/request/SingleRequest.java org/osmdroid/tileprovider/modules/MapTileSqlCacheProvider.java com/mapbox/android/telemetry/ConcurrentQueue.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java org/osmdroid/tileprovider/MapTileCache.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/engine/DecodePa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/DecodePath.java com/mapbox/android/core/crashreporter/CrashReport.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/SourceGenerator.java org/osmdroid/tileprovider/tilesource/TileSourcePolicy.java org/osmdroid/views/overlay/mylocation/MyLocationNewOverlay.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java org/osmdroid/tileprovider/modules/MBTilesFileArchive.java com/mapbox/android/core/location/MapboxFusedLocationEngineImpl.java org/osmdroid/config/DefaultConfigurationProvider.java com/mapbox/android/telemetry/errors/TokenChangeBroadcastReceiver.java org/osmdroid/tileprovider/BitmapPool.java com/mapbox/android/core/MapboxSdkInfoForUserAgentGenerator.java org/osmdroid/tileprovider/util/StorageUtils.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/mapbox/android/telemetry/AlarmReceiver.java com/mapbox/android/telemetry/CertificateBlacklist.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/mapbox/android/telemetry/errors/ErrorReporterJobIntentService.java
	The Application Sensitive		CWE: CWE-532: Insertion of Sensitive	

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/load/data/LocalUriFetcher.java com/journeyapps/barcodescanner/CaptureManager.java com/bumptech/glide/load/model/ByteBufferFileLoader.java org/osmdroid/tileprovider/tilesource/CloudmadeTileSource.java net/danlew/android/joda/ResUtils.java org/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.java com/mapbox/android/telemetry/errors/ErrorReporterClient.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/journeyapps/barcodescanner/camera/CameraManager.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/mapbox/mapboxsdk/log/Logger.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/mapbox/android/core/FileUtils.java timber/log/Timber.java org/osmdroid/views/overlay/infowindow/MarkerInfoWindow.java com/mapbox/android/telemetry/location/LocationUpdatesBroadcastReceiver.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/mapbox/android/core/location/Androi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dLocationEngineImpl.java org/osmdroid/views/overlay/infowindow/BasicInfoWindow.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/mapbox/android/telemetry/TelemetryUtils.java com/caverock/androidsvg/SVGParser.java com/bumptech/glide/load/engine/GlideException.java com/mapbox/android/telemetry/LogUtils.java org/osmdroid/tileprovider/modules/ZipFileArchive.java com/visualizer/amplitude/AudioRecordView.java org/osmdroid/tileprovider/modules/MapTileFilesystemProvider.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/mapbox/android/telemetry/location/LocationCollectionClient.java com/mapbox/android/telemetry/ConfigurationClient.java com/bumptech/glide/load/resource/bitmap/Downsampler.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/metalev/multitouch/controller/MultiTou

NO	ISSUE	SEVERITY	STANDARDS	FILES
				chController.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/manager/RequestManagerFragment.java org/osmdroid/views/overlay/DefaultOverlayManager.java org/osmdroid/views/overlay/infowindow/InfoWindow.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/mapbox/android/telemetry/EventsQueue.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java com/bumptech/glide/load/model/FileLoader.java net/danlew/android/joda/TimeZoneChangedReceiver.java com/mapbox/android/telemetry/Logger.java com/bumptech/glide/manager/RequestTracker.java org/osmdroid/tileprovider/modules/MapTileFileArchiveProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	org/odk/collect/androidshared/system/ExternalFilesUtils.java org/odk/collect/android/injection/config/AppDependencyModule.java org/odk/collect/android/storage/StoragePathProvider.java org/odk/collect/android/backgroundwork/AutoSendTaskSpec.java org/osmdroid/config/DefaultConfigurationProvider.java org/osmdroid/tileprovider/util/StorageUtils.java com/mapbox/mapboxsdk/storage/FileSource.java org/odk/collect/android/application/initialization/upgrade/BeforeProjectsInstallDetector.java org/odk/collect/audiorecorder/AudioRecorderDependencyModule.java
3	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/networknt/schema/SchemaValidatorsConfig.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/Option.java com/networknt/schema/ValidatorState.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/DataCacheKey.java com/networknt/schema/CollectorContext.java org/osmdroid/tileprovider/modules/DatabaseFileArchive.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	org/javarosa/xform/parse/FisherYates.java org/javarosa/xform/parse/ParkMiller.java org/javarosa/core/util/MathUtils.java org/osmdroid/tileprovider/tilesource/BitmapTileSourceBase.java org/javarosa/core/util/PropertyUtils.java j$/util/concurrent/ThreadLocalRandom.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	org/odk/collect/android/utilities/FormDefCache.java org/odk/collect/android/utilities/FileUtils.java com/journeyapps/barcodescanner/CaptureManager.java org/odk/collect/audiorecorder/recorder/RecordingResourceRecorder.java org/mp4parser/boxes/iso14496/part12/MediaDataBox.java
6	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	org/odk/collect/android/utilities/EncryptionUtils.java org/odk/collect/shared/strings/Md5.java org/odk/collect/android/fastexternalitemset/ItemsetDbAdapter.java org/odk/collect/android/configure/qr/CachingQRCodeGenerator.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	org/odk/collect/android/database/forms/FormDatabaseMigrator.java org/odk/collect/android/fastexternalitemset/ItemsetDbAdapter.java org/odk/collect/android/database/instances/InstanceDatabaseMigrator.java org/odk/collect/android/utilities/CustomSQLiteQueryExecutor.java org/odk/collect/android/geo/OsmMBTileSource.java org/osmdroid/tileprovider/modules/SqlTileWriter.java org/odk/collect/android/database/forms/DatabaseFormsRepository.java org/odk/collect/android/externaldata/ExternalSQLiteOpenHelper.java org/odk/collect/android/database/instances/DatabaseInstancesRepository.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	org/odk/collect/android/application/initialization/upgrade/BeforeProjectsInstallDetector.java
9	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	org/odk/collect/android/widgets/items/SelectImageMapWidget.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/mapbox/android/telemetry/CertificatePinnerFactory.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libmapbox-gl.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
2	lib/armeabi-v7a/libmapbox-gl.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['microphone', 'location', 'camera', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
16	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
19	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
a.tile.openstreetmap.org	ok	**IP:** 151.101.121.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
basemap.nationalmap.gov	ok	**IP:** 52.222.158.113 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
b.tile.cloudmade.com	ok	No Geolocation information available.
openptmap.org	ok	**IP:** 88.99.141.112 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map
1.basemaps.cartocdn.com	ok	**IP:** 151.101.122.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
overlay.openstreetmap.nl	ok	**IP:** 93.186.176.173 **Country:** Netherlands **Region:** Overijssel **City:** Enschede **Latitude:** 52.218330 **Longitude:** 6.895830 **View:** Google Map
b.tile.opentopomap.org	ok	**IP:** 131.188.76.144 **Country:** Germany **Region:** Bayern **City:** Erlangen **Latitude:** 49.595612 **Longitude:** 10.994970 **View:** Google Map
demo.getodk.org	ok	**IP:** 198.211.121.145 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
maps.wikimedia.org	ok	**IP:** 185.15.58.240 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	**IP:** 151.101.120.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api-project-322300403941.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
drive.google.com	ok	**IP:** 216.58.214.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
c.tile.cloudmade.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
tiles.openseamap.org	ok	**IP:** 195.37.132.70 **Country:** Germany **Region:** Rheinland-Pfalz **City:** Franken **Latitude:** 50.501240 **Longitude:** 7.234600 **View:** Google Map
c.tile.opentopomap.org	ok	**IP:** 131.188.76.144 **Country:** Germany **Region:** Bayern **City:** Erlangen **Latitude:** 49.595612 **Longitude:** 10.994970 **View:** Google Map
apps.mapbox.com	ok	**IP:** 99.86.91.53 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
forum.getodk.org	ok	**IP:** 45.77.97.47 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
a.tile.cloudmade.com	ok	No Geolocation information available.
a.tile.opentopomap.org	ok	**IP:** 131.188.76.144 **Country:** Germany **Region:** Bayern **City:** Erlangen **Latitude:** 49.595612 **Longitude:** 10.994970 **View:** Google Map
auth.cloudmade.com	ok	**IP:** 23.21.136.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.mapbox.com	ok	**IP:** 13.225.31.125 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
wms.chartbundle.com	ok	**IP:** 138.68.60.210 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** Google Map
www.slf4j.org	ok	**IP:** 83.166.144.67 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.139210 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.201.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.opendatakit.org	ok	**IP:** 13.249.9.122 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
tiles.wmflabs.org	ok	**IP:** 185.15.56.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
c.tile.openstreetmap.org	ok	**IP:** 151.101.121.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
openrosa.org	ok	**IP:** 34.102.136.180 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
b.tile.openstreetmap.org	ok	**IP:** 151.101.121.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.getodk.org	ok	**IP:** 143.204.231.12 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
json-schema.org	ok	**IP:** 172.67.130.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
getodk.org	ok	**IP:** 99.86.91.45 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
tile.stamen.com	ok	**IP:** 151.101.120.249 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://api-project-322300403941.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@getodk.org	org/odk/collect/android/tasks/FormLoaderTask.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Mapbox		https://reports.exodus-privacy.eu.org/trackers/171
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

HARDCODED SECRETS

POSSIBLE SECRETS
"GOOGLE_MAPS_API_KEY" : "AIzaSyBS-JQ-dnaZ_8qsbvSyr_I3rTPFd5fJsYI"
"firebase_database_url" : "https://api-project-322300403941.firebaseio.com"
"google_api_key" : "AIzaSyBS-JQ-dnaZ_8qsbvSyr_I3rTPFd5fJsYI"
"google_crash_reporting_api_key" : "AIzaSyBS-JQ-dnaZ_8qsbvSyr_I3rTPFd5fJsYI"

POSSIBLE SECRETS
"password" : "Password"
"username" : "Username"
"admin_password" : "Administrator-adgangskode"
"password" : "Adgangskode"
"username" : "Brugernavn"
"password" : "پسورد"
"admin_password" : "□□□□□□□□□"
"enter_admin_password" : "□□□□□□□□□□□□□□□□□□□□"
"password" : "□□□□□□"
"server_password" : "□□□□□□□□□□"
"server_requires_auth" : "□□□□□□□□□□□□□"
"show_password" : "□□□□□□□□□"
"username" : "□□□□□□"
"password" : "პაროლი"
"admin_password" : "Admin-Passwort"

POSSIBLE SECRETS
"password" : "Passwort"
"server_password" : "Server-Passwort"
"username" : "Benutzername"
"password" : "Wagwoord"
"username" : "Gebruikersnaam"
"password" : "Salasana"
"server_password" : "Palvelinsalasana"
"username" : "Käyttäjätunnus"
"password" : "■■■■■■■"
"password" : "Пароль"
"password" : "Wachtwoord"
"username" : "Gebruikersnaam"
"password" : "Hasło"
"password" : "Geslo"
"password" : "Kontrasenyas"

POSSIBLE SECRETS
"username" : "Username"
"password" : "[redacted]"
"server_password" : "[redacted]"
"server_requires_auth" : "[redacted]"
"show_password" : "[redacted]"
"username" : "[redacted]"
"password" : "[redacted]"
"password" : "Parola"
"password" : "Fjalëkalimi"
"password" : "[redacted]"
"username" : "[redacted]"
"password" : "Lozinka"
"password" : "Şifre"
"password" : "Heslo"
"password" : "Contraseña"

POSSIBLE SECRETS
"password" : "Salasõna"
"username" : "Kasutajanimi"
"password" : "Password"
"password" : "Slaptažodis"
"password" : "Senha"
"password" : "Пароль"
"password" : "Inombolomfihlo"
"username" : "Igamamfihlo"
"password" : "Nenosiri"
"password" : "■□■□□■□■■■■■□■■"
"show_password" : "■■■■■□■□■□■□"
"username" : "■■■■■□■■■■■■■"
"enter_admin_password" : "ป้อนละหัดผ่านผู้ดวบคุมละบ็บ"
"password" : "ละหัดผ่าน"
"username" : "บันชีผู้ใช้ງาน"

POSSIBLE SECRETS
"password" : "■■■■■■■"
"admin_password" : "□□□□□□"
"enter_admin_password" : "□□□□□□□□"
"password" : "□□"
"server_auth_credentials" : "□□□□□□%s□□□□□□□□□□□□"
"server_requires_auth" : "□□□□□□□□□□"
"show_password" : "□□□□"
"username" : "□□□"
"password" : "Passord"
"username" : "Brukernavn"
"password" : "پتنوم"
"password" : "Thibitisho"
"admin_password" : "Administratörslösenord"
"password" : "Lösenord"
"server_password" : "Serverlösenord"

POSSIBLE SECRETS
"username" : "Användarnamn"
"password" : "Kontrasenyas"
"username" : "Username"
"admin_password" : "[redacted]"
"enter_admin_password" : "[redacted]"
"password" : "[redacted]"
"show_password" : "[redacted]"
"username" : "[redacted]"
"password" : "Contraseña"

PLAYSTORE INFORMATION

Title: ODK Collect

Score: 4.47 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Productivity **Play Store URL:** org.odk.collect.android

Developer Details: ODK, ODK, None, https://getodk.org, support@getodk.org,

Release Date: None **Privacy Policy:** Privacy link

Description:

ODK lets you build powerful forms to collect the data you need wherever it is. Millions of people use ODK to collect data because it lets them: 1. Build powerful forms with photos, GPS points, skip logic, calculations, external datasets, multiple languages, repeating elements, and more. 2. Collect data offline with either the mobile app or

the web app and synchronize that data when an Internet connection is found. 3. Analyze with ease by connecting apps like Excel, Power BI, or R to create live-updating and shareable reports and dashboards. ODK is the standard for social impact organizations because it is proven at global scale, trusted across sectors, and entirely open-source. Join the leading organizations like World Health Organization, Red Cross, Carter Center, and Google who use ODK to make the world a better place. Learn more at https://getodk.org

---

Report Generated by - MobSF v3.5.2 Beta

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.