

ANDROID STATIC ANALYSIS REPORT



Miracle-Ear (4.2.1)

File Name: com.miracleear.mdapp_159.apk

Package Name: com.miracleear.mdapp

Scan Date: Aug. 31, 2025, 5:15 a.m.

App Security Score:

54/100 (MEDIUM RISK)

Grade:

В

Trackers Detection:

3/432

♣ FINDINGS SEVERITY

煮 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
1	16	4	2	1



File Name: com.miracleear.mdapp_159.apk

Size: 136.87MB

MD5: b3a15512ad7994dc9e4a1a53eb68c3a7

SHA1: f0d820cce051c433f1555380cddc6f3a408deb65

SHA256: 944e0f67452da9925a4f73543134f6ccaa2d4941c16eaa2b82ebc621e58584b0

i APP INFORMATION

App Name: Miracle-Ear

Package Name: com.miracleear.mdapp

Main Activity: crc644b81debddfe1fda9.SplashActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 4.2.1
Android Version Code: 159

APP COMPONENTS

Activities: 19 Services: 14 Receivers: 18 Providers: 7

Exported Activities: 0 Exported Services: 2 Exported Receivers: 3 Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: O=Amplifon

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2018-03-28 16:39:46+00:00 Valid To: 2048-03-20 16:39:46+00:00

Issuer: O=Amplifon Serial Number: 0x7c8f8de6 Hash Algorithm: sha256 md5: 8aaaf72c27dcd7f56194d59a77510e87

sha1: 4911235ef6c77ba6dfa7c1044ec67d602bc2a32b

sha256: 49583c3b8cdb7dc4de7cb5f97101436afd194b92b5d58b9549a6858be98a2668

sha512:9f9a8a636550254c1b007ddd397377792da23ea804e6e013c31e4aeeb599063d05fb3c02daf65a32a4372500f58363175f3af0e1ec57561cd3881d3df4f3e0e1

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 97000d8dff2c7a62dedab17ac69f912da69987aab4f564d2e6d9695d7864c39d

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device- supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
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.
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.miracleear.mdapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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	normal	permission defined by google	A custom permission defined by Google.

ক্ল APKID ANALYSIS

FILE	DETAILS	
b3a15512ad7994dc9e4a1a53eb68c3a7.apk	FINDINGS	DETAILS
взатээтгайг ээнисэсна тазэсвоосзат.арк	Anti-VM Code	possible VM check

FILE	DETAILS	
	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check network operator name check
classes.dex	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
	Compiler	r8 without marker (suspicious)
	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	That Bessay code	Build.MODEL check
classes3.dex	Anti-VM Code	Build.MODEL CHECK Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check possible VM check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS		
	FINDINGS	DETAILS	
classes4.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check	
classes5.dex	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes6.dex	Anti-VM Code	Build.HARDWARE check possible VM check	
	Compiler	r8 without marker (suspicious)	
	FINDINGS	DETAILS	
classes7.dex	Anti-VM Code	Build.MANUFACTURER check Build.HARDWARE check	
	Compiler	r8 without marker (suspicious)	

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

Q MANIFEST ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning This application can be installed on an older version of android that has multiple vulnerabilities. Supply version => 10, API 29 to receive reasonable security updates.	
2	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 8 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/Event.java com/adobe/marketing/mobile/Event.java com/adobe/marketing/mobile/Lifecycle.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/Signal.java com/adobe/marketing/mobile/UserProfile.java com/adobe/marketing/mobile/VatoV5Migration.java com/adobe/marketing/mobile/VistorID.java com/adobe/marketing/mobile/analytics/internal/AnalyticsDatabase.java com/adobe/marketing/mobile/analytics/internal/AnalyticsHitProcessor.j ava com/adobe/marketing/mobile/analytics/internal/AnalyticsState.java com/adobe/marketing/mobile/analytics/internal/ContextDataUtil.java com/adobe/marketing/mobile/analytics/internal/ContextDataUtil.java com/adobe/marketing/mobile/internal/configuration/ConfigurationDow nloader.java com/adobe/marketing/mobile/internal/configuration/ConfigurationDow nloader.java com/adobe/marketing/mobile/internal/configuration/ConfigurationRules Manager.java com/adobe/marketing/mobile/internal/configuration/ConfigurationState Manager.java com/adobe/marketing/mobile/internal/configuration/ConfigurationState Manager.java com/adobe/marketing/mobile/internal/eventhub/EventHub\$registerRes ponseListener\$1.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/EventHub.java com/adobe/marketing/mobile/internal/eventhub/ExtensionContainer.jav a com/adobe/marketing/mobile/internal/eventhub/ExtensionContainer.jav a com/adobe/marketing/mobile/internal/eventhub/ExtensionContainer.jav

NO	ISSUE	SEVERITY	STANDARDS	ainer.java
				com/adobe/marketing/mobile/internal/eventhub/history/AndroidEventH istory.java com/adobe/marketing/mobile/internal/eventhub/history/AndroidEventH istoryDatabase.java com/adobe/marketing/mobile/internal/util/FileUtils.java com/adobe/marketing/mobile/internal/util/SQLiteDatabaseHelper.java com/adobe/marketing/mobile/internal/util/StringEncoder.java com/adobe/marketing/mobile/launch/rulesengine/HistoricalEventsQuer yingKt.java com/adobe/marketing/mobile/launch/rulesengine/LaunchRulesConsequ ence.java com/adobe/marketing/mobile/launch/rulesengine/LaunchTokenFinder.j ava com/adobe/marketing/mobile/launch/rulesengine/LaunchTokenFinder.j ava com/adobe/marketing/mobile/launch/rulesengine/download/RulesLoad er.java com/adobe/marketing/mobile/launch/rulesengine/json/GroupCondition.java com/adobe/marketing/mobile/launch/rulesengine/json/GroupCondition.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONCondition.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONCondition.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONRule.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONRulesParse r.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONRulesParse r.java com/adobe/marketing/mobile/liecycle/LifecycleExtension.java com/adobe/marketing/mobile/lifecycle/LifecycleExtension.java com/adobe/marketing/mobile/lifecycle/LifecycleExtension.java com/adobe/marketing/mobile/lifecycle/LifecycleExtension.java com/adobe/marketing/mobile/lifecycle/LifecycleSsaion.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mobile/lifecycle/LifecycleState.java com/adobe/marketing/mob
				com/adobe/marketing/mobile/services/HttpConnectionHandler.java com/adobe/marketing/mobile/services/LocalDataStoreService.java com/adobe/marketing/mobile/services/MessagingDelegate.java com/adobe/marketing/mobile/services/NetworkService.java com/adobe/marketing/mobile/services/SQLiteDataQueue.java com/adobe/marketing/mobile/services/SharedPreferencesNamedCollect ion.iava

NO	ISSUE	SEVERITY	STANDARDS	com/adobe/marketing/mobile/services/TLSSocketFactory.java
NO	ISSUE	SEVERITY	STANDARDS	com/adobe/marketing/mobile/services/TLSSocketFactory.java Enfadiobe/marketing/mobile/services/internal/caching/CacheFileMana ger.java com/adobe/marketing/mobile/services/internal/caching/FileCacheServic e.java com/adobe/marketing/mobile/services/ui/AEPMessage.java com/adobe/marketing/mobile/services/ui/FloatingButtonManager.java com/adobe/marketing/mobile/services/ui/FloatingButtonView.java com/adobe/marketing/mobile/services/ui/FloatingButtonView.java com/adobe/marketing/mobile/services/ui/FloatingButtonView.java com/adobe/marketing/mobile/services/ui/MessageFragment.java com/adobe/marketing/mobile/services/ui/MessageWebViewClient.java com/adobe/marketing/mobile/services/ui/MessageWebViewUtil.java com/adobe/marketing/mobile/services/ui/MessageWebViewUtil.java com/adobe/marketing/mobile/services/ui/internal/MessagesMonitor.jav a com/adobe/marketing/mobile/services/ui/internal/MessagesMonitor.java com/adobe/marketing/mobile/signal/internal/SignalExtension.java com/adobe/marketing/mobile/userprofile/JSONUtils.java com/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/userprofile/Jsorus/adobe/marketing/mobile/u
				com/github/mikephil/charting/charts/HorizontalBarChart.java
				com/github/mikephil/charting/data/PieData.java com/github/mikephil/charting/data/PieData.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/github/sarxos/webcam/WebcamExceptionHandler.java
				com/github/sarxos/webcam/webcamExceptionHandler.java com/github/sarxos/webcam/WebcamViewer.java com/github/sarxos/webcam/log/WebcamLogConfigurator.java com/kenai/jffi/Main.java com/sonova/firmwareupdate/internal/Update\$update\$20.java

NO ISSUE	SEVERITY	STANDARDS	com/sonova/firmwareupdate/internal/Update.java FILES com/sonova/firmwareupdate/internal/helpers/LogServiceImpl.java
			com/sonova/health/component/service/sync/DataSyncServiceInternalImpl.java com/sonova/health/component/service/sync/response/ChargingPeriods DeviceLog,java com/sonova/health/component/service/sync/response/HeartRateDevice Log,java com/sonova/health/component/service/sync/response/IntervalDeviceLog,java com/sonova/health/component/service/sync/response/IntervalDeviceLog,java com/sonova/health/component/service/sync/response/IntervalDeviceLog,java com/sonova/health/features/HealthFeatureLog,java com/sonova/health/features/HealthFeatureLog,java com/sonova/health/features/provider/impl/LogRequiredObjectsProvider java com/sonova/health/model/log/HealthLog,java com/sonova/health/model/log/HealthLog,java com/sonova/mobilecore/LogServiceImpl.java com/sonova/mobilecsdk/common/internal/ExtensionsKt.java com/sonova/mobilesdk/common/internal/ExtensionsKt.java com/sonova/mobilesdk/common/internal/ExtensionsKt.java com/sonova/mobilesdk/requiredinterface/internal/DefaultLogger,java com/sonova/mobilesdk/requiredinterface/internal/DefaultLogger,java com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/mobilesdk/services/remotecontrol/mobilecore/RCDeviceImpl.jiava com/sonova/remotesupport/fommon/error/RemoteSupportError.java com/sonova/remotesupport/romanager/ds/conference/AudioRecordSourceWOHeadsetRouting,java com/sonova/remotesupport/manager/ds/conference/AudioRecordSourceWOHeadsetRouting,java com/sonova/remotesupport/manager/ds/conference/CupoutManager.java com/sonova/remotesupport/model/activepassiveobserver/RSActivePass veObserverModel.java com/sonova/remotesupport/model/conference/ConferenceAudioVideo.java dom/sonova/remotesupport/model/conference/ConferenceAudioVideo.java dom/sonova/remotesupport/mode

NO	ISSUE	SEVERITY	STANDARDS	dutrovorg/jctools/maps/concurrent/dutrable-java edtreg/org/jctools/maps/NonBlockingHashMap.java ddtrot/org/jctools/maps/NonBlockingHashMapLong.java
				ddtrot/org/jctools/maps/NonBlockingldentityHashMap.java
				ddtrot/org/jctools/maps/NonBlockingSetInt.java
				fm/liveswitch/Asn1Any.java
				fm/liveswitch/Asn1ObjectIdentifier.java
				fm/liveswitch/Asn1Set.java
				fm/liveswitch/AudioBuffer.java
				fm/liveswitch/AudioEncoder.java
			CWE: CWE-532: Insertion of Sensitive Information into Log	fm/liveswitch/AudioLevelContext.java
	The App logs information. Sensitive information	info	File	fm/liveswitch/AudioStream.java
	should never be logged.		OWASP MASVS: MSTG-STORAGE-3	fm/liveswitch/AudioTrack.java
			OWNER WINDOWS WISH OF STORY REED	fm/liveswitch/Binary.java
				fm/liveswitch/BundleDescriptionManager.java
				fm/liveswitch/ByeControlFrame.java
				fm/liveswitch/ByteCollection.java
				fm/liveswitch/Certificate.java
				fm/liveswitch/Channel.java
				fm/liveswitch/Client.java
				fm/liveswitch/Connection.java
				fm/liveswitch/ConnectionBase.java
				fm/liveswitch/ConsoleLogProvider.java
				fm/liveswitch/DataChannelBase.java
				fm/liveswitch/DataChalmerbase.java
				fm/liveswitch/DataStream.java
				· ·
				fm/liveswitch/DnsRequest.java
				fm/liveswitch/DtlsBouncyCastleClient.java
				fm/liveswitch/DtlsBouncyCastleClientAuthentication.java
				fm/liveswitch/DtlsBouncyCastleClientProtocol.java
				fm/liveswitch/DtlsBouncyCastleServer.java
				fm/liveswitch/DtlsBouncyCastleServerProtocol.java
				fm/liveswitch/DtlsCertificate.java
				fm/liveswitch/DtlsTransport.java
				fm/liveswitch/FakeAudioSource.java
				fm/liveswitch/FakeVideoSource.java
				fm/liveswitch/FecContext.java
				fm/liveswitch/FecReceiver.java
				fm/liveswitch/FileAssistant.java
				fm/liveswitch/FrameRatePipe.java
				fm/liveswitch/Global.java
				fm/liveswitch/HttpTransfer.java
				fm/liveswitch/IceCandidate.java
				fm/liveswitch/IceDatagramSocketManager.java
				fm/liveswitch/IceGatherer.java
				fm/liveswitch/IceLocalRelayedCandidate.java
				fm/liveswitch/IceSocketManager.java
				fm/liveswitch/IceTransport.java
				fm/liveswitch/ImageScalePipe.java
				fm/liveswitch/ImageSizePipe.java
				fm/liveswitch/Invitation.java
				fm/liveswitch/LayoutManager.java
				fm/liveswitch/LocalMedia.java
		İ		fm/liveswitch/LocalMediaBase.java

				tm/liveswitch/ivianagedConnection.java
10	ISSUE	SEVERITY	STANDARDS	FT/Liveswitch/Media.java
				fm/liveswitch/MediaDescriptionManager.java
				fm/liveswitch/MediaPipe.java
				fm/liveswitch/MediaRecorder.java
				fm/liveswitch/MediaSink.java
				fm/liveswitch/MediaSource.java
				fm/liveswitch/MediaStream.java
				fm/liveswitch/MediaStreamBase.java
				fm/liveswitch/MediaTrack.java
				fm/liveswitch/MediaTransport.java
				fm/liveswitch/PathUtility.java
				fm/liveswitch/PeerConnectionOffer.java
				fm/liveswitch/Promise.java
				fm/liveswitch/PromiseBase.java
				fm/liveswitch/ReliableChannel.java
				fm/liveswitch/ReliableTransport.java
				fm/liveswitch/RsaCrypto.java
				fm/liveswitch/RtcLocalMedia.java
				fm/liveswitch/RtcRemoteMedia.java
				fm/liveswitch/RtcpPacket.java
				fm/liveswitch/RtpListener.java
				fm/liveswitch/RtpPacket.java
				fm/liveswitch/RtpTransport.java
				fm/liveswitch/RtpUnknownHeaderExtensionElement.java
				fm/liveswitch/SctpChunk.java
				fm/liveswitch/SctpChunkListChunkParameter.java
				fm/liveswitch/SctpCookieAckChunk.java
				fm/liveswitch/SctpCookieEchoChunk.java
				fm/liveswitch/SctpCookiePreservativeChunkParameter.java
				fm/liveswitch/SctpCookieReceivedWhileShuttingDown.java
				fm/liveswitch/SctpDataChunk.java
				fm/liveswitch/SctpDataQueue.java
				fm/liveswitch/SctpErrorChunk.java
				fm/liveswitch/SctpForwardTsnSupportedChunkParameter.java
				fm/liveswitch/SctpGenericChunk.java
				fm/liveswitch/SctpGenericChunkParameter.java
				fm/liveswitch/SctpHeartbeatAckChunk.java
				fm/liveswitch/SctpHeartbeatChunk.java
				fm/liveswitch/SctpHeartbeatInfoChunkParameter.java
				fm/liveswitch/SctpHostNameAddressChunkParameter.java
				fm/liveswitch/SctpIPv4ChunkParameter.java
				fm/liveswitch/SctpInitAckChunk.java
				fm/liveswitch/SctpInitChunk.java
				fm/liveswitch/SctpInnerSctpTransport.java
				fm/liveswitch/SctpInvalidMandatoryParameter.java
				fm/liveswitch/SctpInvalidStreamIdentifier.java
				fm/liveswitch/SctpMissingMandatoryParameter.java
				fm/liveswitch/SctpNoUserData.java
				fm/liveswitch/SctpOutOfResource.java
				fm/liveswitch/SctpPacket.java
				fm/liveswitch/SctpPadChunkParameter.java
				fm/liveswitch/SctpProtocolViolation.java
				fm/liveswitch/SctpRandomChunkParameter.java
		I		

ISSUE	SEVERITY		
	SEVERIII	STANDARDS	ፑተሂ ኲି §switch/SctpRestartOfAnAssociationWithNewAddresses.java
			fm/liveswitch/SctpStaleCookieError.java
			fm/liveswitch/SctpStateCookieChunkParameter.java
			fm/liveswitch/SctpSupportedAddressTypesChunkParameter.java
			fm/liveswitch/SctpSupportedExtensionsChunkParameter.java
			fm/liveswitch/SctpTlvParameter.java
			fm/liveswitch/SctpTransmissionControlBlock.java
			fm/liveswitch/SctpTransport.java
			fm/liveswitch/SctpUnrecognizedChunkType.java
			fm/liveswitch/SctpUnrecognizedParameterChunkParameter.java
			fm/liveswitch/SctpUnrecognizedParameters.java
			fm/liveswitch/SctpUnresolvableAddress.java
			fm/liveswitch/SctpUserInitiatedAbort.java
			fm/liveswitch/SendQueue.java
			fm/liveswitch/ServerConnection.java
			fm/liveswitch/SessionDescriptionManager.java
			fm/liveswitch/SignallingClient.java
			fm/liveswitch/SignallingClientBase.java
			fm/liveswitch/SoundReframerContext.java
			fm/liveswitch/SrtpContext.java
			fm/liveswitch/Stream.java
			fm/liveswitch/StreamBase.java
			,
			fm/liveswitch/StunServer.java
			fm/liveswitch/TcpSocket.java
			fm/liveswitch/TlsCertificate.java
			fm/liveswitch/TransportAddress.java
			fm/liveswitch/TurnAllocation.java
			fm/liveswitch/TurnServer.java
			fm/liveswitch/TurnUdpAllocation.java
			fm/liveswitch/Unhandled.java
			fm/liveswitch/VideoBuffer.java
			fm/liveswitch/VideoDecoder.java
			fm/liveswitch/VideoEncoder.java
			fm/liveswitch/VideoPipe.java
			fm/liveswitch/VideoSink.java
			fm/liveswitch/VideoSource.java
			fm/liveswitch/VideoStream.java
			fm/liveswitch/VideoTrack.java
			fm/liveswitch/VirtualNatMapping.java
			fm/liveswitch/WebSocketWebRequestTransfer.java
			fm/liveswitch/X509TbsCertificate.java
			fm/liveswitch/android/AudioRecordSource.java
			fm/liveswitch/android/AudioRecordSource2.java
			fm/liveswitch/android/Camera2Source.java
			fm/liveswitch/android/CameraPreview.java
			fm/liveswitch/android/CameraSource.java
			fm/liveswitch/android/ImageViewSink.java
			fm/liveswitch/android/LayoutManager.java
			fm/liveswitch/android/LogProvider.java
			fm/liveswitch/android/MediaCodecDecoder.java
			fm/liveswitch/android/MediaCodecEncoder.java
			*
			fm/liveswitch/android/MediaCodecUtility.java fm/liveswitch/android/MediaProjectionSource.java

		I		fm/liveswitch/android/OpenGLSink.java
NO	ISSUE	SEVERITY	STANDARDS	Fh//Fsswitch/android/ViewSource.java
				fm/liveswitch/audioprocessing/Native.java
				fm/liveswitch/audioprocessing/Utility.java
				fm/liveswitch/dtmf/Receiver.java
				fm/liveswitch/dtmf/Sender.java
				fm/liveswitch/h264/Packet.java
				fm/liveswitch/h265/Packet.java
				fm/liveswitch/ivf/VideoSink.java
				fm/liveswitch/java/ImageViewLayoutManager.java
				fm/liveswitch/java/LayoutManager.java
				fm/liveswitch/java/ScreenSource.java
				fm/liveswitch/java/SoundSink.java
				fm/liveswitch/java/SoundSource.java
				fm/liveswitch/java/Utility.java
				fm/liveswitch/java/sarxos/VideoSource.java
				fm/liveswitch/matroska/Audio.java
				· ·
				fm/liveswitch/matroska/AudioSource iava
				fm/liveswitch/matroska/AudioSource.java
				fm/liveswitch/matroska/BlockGroup.java
				fm/liveswitch/matroska/Cluster.java
				fm/liveswitch/matroska/ContentCompression.java
				fm/liveswitch/matroska/ContentEncoding.java
				fm/liveswitch/matroska/ContentEncodings.java
				fm/liveswitch/matroska/Ebml.java
				fm/liveswitch/matroska/File.java
				fm/liveswitch/matroska/Seek.java
				fm/liveswitch/matroska/SeekHead.java
				fm/liveswitch/matroska/Segment.java
				fm/liveswitch/matroska/SegmentInfo.java
				fm/liveswitch/matroska/Track.java
				fm/liveswitch/matroska/TrackEntry.java
				fm/liveswitch/matroska/Video.java
				fm/liveswitch/matroska/VideoSink.java
				fm/liveswitch/matroska/VideoSource.java
				fm/liveswitch/ogg/AudioSink.java
				fm/liveswitch/openh264/Encoder.java
				fm/liveswitch/openh264/Native.java
				fm/liveswitch/opus/Decoder.java
				fm/liveswitch/opus/Encoder.java
				fm/liveswitch/opus/Native.java
				fm/liveswitch/opus/Utility.java
				fm/liveswitch/sdp/DirectionAttribute.java
				fm/liveswitch/sdp/rtcp/FeedbackAttribute.java
				fm/liveswitch/vp8/Packet.java
				fm/liveswitch/vpx/Encoder.java
				fm/liveswitch/vpx/Native.java
				fm/liveswitch/vpx/Utility.java
				fm/liveswitch/wave/AudioSink.java
				fm/liveswitch/yuv/Native.java
				fm/liveswitch/yuv/Utility.java
				fm/liveswitch/yuv4mpeg/VideoSink.java
				fm/liveswitch/yuv4mpeg/VideoSource.java
				, , , ,

NO	ISSUE	SEVERITY	STANDARDS	org/bridj/demangling/Demangler.java State
				anglan ymaqana angana
				com/adobe/marketing/mobile/DataMarshaller.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/NotificationDismissalHandler.java com/adobe/marketing/mobile/UserProfile.java com/adobe/marketing/mobile/V4ToV5Migration.java com/adobe/marketing/mobile/analytics/internal/AnalyticsConstants.java com/adobe/marketing/mobile/identity/IdentityConstants.java com/adobe/marketing/mobile/internal/AppResourceStore.java com/adobe/marketing/mobile/internal/CoreConstants.java com/adobe/marketing/mobile/internal/configuration/ConfigurationExte nsion.java com/adobe/marketing/mobile/internal/configuration/ConfigurationState Manager.java com/adobe/marketing/mobile/launch/rulesengine/json/JSONDefinition.j
				ava com/adobe/marketing/mobile/lifecycle/LifecycleConstants.java com/adobe/marketing/mobile/services/ui/AndroidUlService.java com/adobe/marketing/mobile/userprofile/UserProfileConstants.java com/datadog/android/log/internal/LogsFeature.java com/datadog/android/rum/internal/RumFeature.java com/datadog/android/rum/internal/domain/scope/ExternalResourceTim ingsKt.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/android/rum/internal/domain/scope/RumSessionScope.ja
				va com/datadog/android/sessionreplay/internal/SessionReplayFeature.java com/datadog/android/sessionreplay/internal/domain/RequestBodyFact ory.java com/datadog/android/tracing/TracingInterceptor.java com/datadog/android/v2/api/RequestFactory.java com/datadog/android/webview/internal/MixedWebViewEventConsumer .java
				com/datadog/opentracing/DDSpanContext.java com/datadog/opentracing/propagation/B3HttpCodec.java com/datadog/opentracing/propagation/B3MHttpCodec.java com/datadog/opentracing/propagation/DatadogHttpCodec.java com/datadog/opentracing/propagation/HaystackHttpCodec.java com/datadog/opentracing/propagation/W3CHttpCodec.java com/datadog/trace/api/Config.java com/datadog/trace/common/sampling/RateByServiceSampler.java
				com/sonova/communicationtypes/generated/ActiveScenarioContext.java com/sonova/communicationtypes/generated/ActiveSituation.java com/sonova/communicationtypes/generated/ActivityTuningSecret.java com/sonova/communicationtypes/generated/Automat.java com/sonova/communicationtypes/generated/BinauralConfig.java com/sonova/communicationtypes/generated/DataLoggingSlotAdjustme nt.java com/sonova/communicationtypes/generated/DataLoggingSlotCorrection .java

NO	ISSUE	SEVERITY	STANDARDS	com/sonova/communicationtypes/generated/DataLoggingSlotTmicUsag FileS com/sonova/communicationtypes/generated/DataLoggingSlotUnlock.iay
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	a com/sonova/communicationtypes/generated/DataLoggingSlotUsage.jav a com/sonova/communicationtypes/generated/DirectActivationAction.java com/sonova/communicationtypes/generated/DirectActivationActionV2.java com/sonova/communicationtypes/generated/DynamicServiceStateDescriptor.java com/sonova/communicationtypes/generated/FittingDeltaIndex.java com/sonova/communicationtypes/generated/FittingDeltaIndex.java com/sonova/communicationtypes/generated/HdScenarioContext.java com/sonova/communicationtypes/generated/HdScenarioContext.java com/sonova/communicationtypes/generated/HdSituationCluster.java com/sonova/communicationtypes/generated/HdSituationCluster.java com/sonova/communicationtypes/generated/HdSituationCluster.java com/sonova/communicationtypes/generated/SetBeamformerStrengthO verrideEnableAction.java com/sonova/communicationtypes/generated/SetBinauralBeamformerEnableAction.java com/sonova/communicationtypes/generated/SetInputGainDelta20Actio n.java com/sonova/communicationtypes/generated/SetInputGainDelta20Actio n.java com/sonova/communicationtypes/generated/SetRelativeStrengthAction.java com/sonova/communicationtypes/generated/SetRelativeStrengthAction.java com/sonova/communicationtypes/generated/UsageLoggingSlotAllocatio n.java com/sonova/datalake/client/infrastructure/ApiClient.java com/sonova/datalake/client/models/ComponentsHSScreenerldentification010.java com/sonova/datalake/client/models/Consent.java com/sonova/firmwareupdate/lupdateConfiguration.java com/sonova/firmwareupdate/lupdateConfiguration.java com/sonova/firmwareupdate/lupdateConfiguration.java com/sonova/firmwareupdate/internal/FileSystemInfoXMLParser.java com/sonova/firmwareupdate/internal/FileSystemInfoXMLParser.java com/sonova/health/cache/encity/DeviceDescriptionEntity.java com/sonova/health/features/InfoDataXmlParser.java com/sonova/health/features/InfoDataXmlParser.java com/sonova/health/features/InfoDataXmlParser.java com/sonova/health/features/InfoDataXmlParser.java com/sonova/health/model/Cache/encytentity/DeviceDescriptionEntity.jav

NO	ISSUE	SEVERITY	STANDARDS	ava Fult Sonova/mobilesdk/requiredinterface/LogData.java com/sonova/mobilesdk/services/common/internal/PairedDeviceContext
				Idl.ogger.java com/sonova/mobilesdk/services/common/internal/PairedDeviceStorage .java com/sonova/mobilesdk/services/remotesupport/RemoteSupportConfigu ration.java com/sonova/monitoring/MOActivityDataConsentRecord.java com/sonova/platformabstraction/embeddedcontents/EmbeddedContent sProvider.java com/sonova/remotecontrol/BinauralStorageKeyPair.java com/sonova/remotecontrol/ProgramInstanceKey.java com/sonova/remotecontrol/StorageKeyPair.java com/sonova/remotecontrol/fittingstateclient/clientlibrary/OAuth2ClientC redentialsTokenConfiguration.java com/sonova/remotecontrol/fittingstateclient/clientlibrary/awaitedresour ce/PollingAwaitedResourceConfiguration.java com/sonova/remotecontrol/fittingstateclient/fittingstateclient/FittingStat eClientConfiguration.java com/sonova/remotesupport/common/parameters/ParameterDefinition.j ava com/sonova/remotesupport/common/preferences/PairedDevicesPrefer ences.java com/sonova/remotesupport/manager/ds/conference/Signalling.java com/sonova/remotesupport/manager/ds/conference/PresenceResponse.ja va com/sonova/remotesupport/manager/liveswitch/configuration/IceServe r.java ddtrot/dd/trace/bootstrap/instrumentation/api/InstrumentationTags.jav a ddtrot/dd/trace/bootstrap/instrumentation/api/InstrumentationTags.jav a ddtrot/dd/trace/core/propagation/BatdogHttpCodec.java ddtrot/dd/trace/core/propagation/BaHttpCodec.java ddtrot/dd/trace/core/propagation/BaHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHatshMap.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHttpCodec.java ddtrot/dd/trace/core/propagation/MatgogHatshMap.java ddtrot/dd/trace/core/propagation/BashMap.java ddtrot/dd/trace/lambda/LambdaHandler.java ddtrot/dd/trace/lambda/LambdaHandler.java ddtrot/do/trace
3	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	mono/android/content/ClipboardManager_OnPrimaryClipChangedListen erImplementor.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	com/adobe/marketing/mobile/services/ui/AEPMessage.java com/datadog/android/tracing/AndroidTracer.java com/datadog/opentracing/DDTracer.java com/datadog/opentracing/StringCachingBigInteger.java com/otohub/ap/utils/PeripheralAddressUtils.java com/sonova/mobilecore/MCCallbackImpl.java fm/liveswitch/RandomExtensions.java fm/liveswitch/Randomizer.java fm/liveswitch/WebSocket.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fm/liveswitch/BundleDescriptionManager.java fm/liveswitch/HexDump.java fm/liveswitch/MediaDescriptionRequirements.java fm/liveswitch/MediaDescriptionManager.java fm/liveswitch/SessionDescriptionManager.java fm/liveswitch/Stream.java fm/liveswitch/TcpSocket.java fm/liveswitch/TransportAddress.java fm/liveswitch/UdpSocket.java fm/liveswitch/WebSocket.java fm/liveswitch/WebSocket.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/adobe/marketing/mobile/internal/util/StringEncoder.java com/sonova/mobilesdk/services/common/PairedDevice.java com/sonova/mobilesdk/services/common/Uuid5Generator.java fm/liveswitch/RsaCrypto.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/github/sarxos/webcam/WebcamLock.java com/kenai/jffi/internal/StubLoader.java com/sonova/datalake/client/infrastructure/ApiClient.java ddtrot/jnr/unixsocket/Common.java org/bridj/Platform.java
8	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/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/sonova/remotesupport/manager/ds/conference/LocalMedia.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/lyft/kronos/AndroidClockFactory.java com/sonova/mobilecore/TransactionalityBugService.java com/sonova/mobilesdk/SonovaMobile.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/sonova/firmwareupdate/internal/network/FirmwareUpdateApi.java com/sonova/mobilesdk/common/internal/network/RetrofitManager.jav a

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	com/adobe/marketing/mobile/internal/eventhub/history/AndroidEventH istoryDatabase.java com/adobe/marketing/mobile/internal/util/SQLiteDatabaseHelper.java
12	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	fm/liveswitch/AesCounterContext.java
13	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/pierfrancescosoffritti/androidyoutubeplayer/core/player/views/We bViewYouTubePlayer.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	------------------	----	-----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	sparcv9- SunOS/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,-z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/sw/lib/64 high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/sw/lib/64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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
2	x86_64-SunOS/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/lib/64:/usr/lib/64:/usr/sfw/lib/64 high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/lib/64:/usr/lib/64:/usr/sfw/lib/64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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
3	sparcv9-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64- FreeBSD/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,-z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64- DragonFlyBSD/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable, Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	/usr/lib/gcc80 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	mips64el- Linux/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64-Linux/libjffi- 1.2.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	i386-Linux/libjffi- 1.2.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64- OpenBSD/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	s390x-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	aarch64-Linux/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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: ['sprintf_chk', 'snprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	i386-SunOS/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/usr/ccs/lib:/lib:/usr/lib:/usr/sfw/lib high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/usr/ccs/lib:/lib:/usr/lib:/usr/sfw/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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
14	aarch64- FreeBSD/libjffi-1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	ppc64-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	/opt/at7.0/lib64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	ppc64le-Linux/libjffi- 1.2.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.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,-z,now to enable full RELRO.	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: ['sprintf_chk', 'snprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	sparcv9- SunOS/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,-z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/sw/lib/64 high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/sw/lib/64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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_64-SunOS/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/lib/64:/usr/lib/64:/usr/sfw/lib/64 high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/lib/64:/usr/lib/64:/usr/sfw/lib/64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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
19	sparcv9-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86_64- FreeBSD/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86_64- DragonFlyBSD/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,-z,now to enable full RELRO and only - z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	mips64el- Linux/libjffi-1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64-Linux/libjffi- 1.2.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	i386-Linux/libjffi- 1.2.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86_64- OpenBSD/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	s390x-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	aarch64-Linux/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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: ['sprintf_chk', 'snprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	arm-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,-z,now to enable full RELRO and only - z,relro to enable partial RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	i386-SunOS/libjffi- 1.2.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non- executable. Use option noexecstack or -z noexecstack to mark stack as 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	/usr/ccs/lib:/lib:/usr/lib:/usr/sfw/lib high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option -rpath to remove RPATH.	/usr/ccs/lib:/lib:/usr/lib:/usr/sfw/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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
30	aarch64- FreeBSD/libjffi-1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	ppc64-Linux/libjffi- 1.2.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option - z,relro,- z,now to enable full RELRO and only - z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	/opt/at7.0/lib64 high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	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.	False Warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	ppc64le-Linux/libjffi- 1.2.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.	Partial RELRO Warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.	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: ['sprintf_chk', 'snprintf_chk']	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
		•		

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	ddtrot/dd/common/socket/TunnelingUnixSocket.java ddtrot/dd/common/socket/UnixDomainSocketFactory.java ddtrot/dd/trace/core/StatusLogger.java fm/liveswitch/TcpSocket.java
00163	Create new Socket and connecting to it	socket	com/adobe/marketing/mobile/services/HttpConnectionHandler.java com/sonova/platformabstraction/web/HttpClient.java ddtrot/dd/common/socket/TunnelingUnixSocket.java ddtrot/dd/common/socket/UnixDomainSocketFactory.java ddtrot/dd/trace/core/StatusLogger.java ddtrot/jnr/unixsocket/UnixDatagramSocket.java ddtrot/jnr/unixsocket/UnixSocket.java ddtrot/jnr/unixsocket/UnixSocket.java ddtrot/jnr/unixsocket/UnixSocketChannel.java fm/liveswitch/TcpSocket.java
00022	Open a file from given absolute path of the file	file	com/adobe/marketing/mobile/internal/util/FileUtils.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/datadog/android/rum/internal/ndk/DatadogNdkCrashHandler.java com/datadog/android/v2/core/internal/storage/Batchld.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/Chart.java com/kenai/jffl/internal/StubLoader.java com/sonova/health/db/DBUtils.java ddtrot/jnr/ffi/Library.java ddtrot/jnr/ffi/Platform.java ddtrot/jnr/posix/JavaFileStat.java ddtrot/jnr/posix/JavaFileStat.java ddtrot/jnr/posix/lavaFileStat.java fm/liveswitch/Global.java fm/liveswitch/PathUtility.java org/bridj/Platform.java
00209	Get pixels from the latest rendered image	collection	fm/media/NativeCamera2Source.java fm/media/NativeMediaProjectionSource.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/adobe/marketing/mobile/internal/util/FileUtils.java com/adobe/marketing/mobile/launch/rulesengine/download/RulesZipProcessingHelper.java com/adobe/marketing/mobile/services/internal/caching/FileCacheResult.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java com/github/sarxos/webcam/WebcamLock.java com/github/sarxos/webcam/log/WebcamLogConfigurator.java com/kenai/jffi/internal/StubLoader.java ddtrot/jnr/ffi/provider/jffi/NativeLibrary.java ddtrot/org/objectweb/asm/util/CheckClassAdapter.java ddtrot/org/objectweb/asm/util/Printer.java okio/Okio_JvmOkioKt.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/sonova/platformabstraction/web/HttpClient.java fm/liveswitch/HttpWebRequestTransfer.java
00089	Connect to a URL and receive input stream from the server	command network	com/sonova/platformabstraction/web/HttpClient.java fm/liveswitch/HttpWebRequestTransfer.java
00109	Connect to a URL and get the response code	network command	com/sonova/platformabstraction/web/HttpClient.java fm/liveswitch/HttpWebRequestTransfer.java
00094	Connect to a URL and read data from it	command network	fm/liveswitch/HttpWebRequestTransfer.java
00108	Read the input stream from given URL	network command	fm/liveswitch/HttpWebRequestTransfer.java
00102	Set the phone speaker on	command	com/otohub/oce/StandardRTCManager.java fm/media/NativeAudioRecordSource.java
00039	Start a web server	control network	fm/liveswitch/TcpSocket.java
00088	Create a secure socket connection to the given host address	command network	fm/liveswitch/TcpSocket.java
00047	Query the local IP address	network collection	fm/liveswitch/TcpSocket.java fm/liveswitch/UdpSocket.java
00148	Create a socket connection to the given host address	network command	fm/liveswitch/TcpSocket.java
00056	Modify voice volume	control	org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	fm/media/NativeCameraSource.java org/webrtc/Camera1Session.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/sonova/platformabstraction/web/HttpClient.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/services/DeviceInfoService.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/AndroidUlService.java
00091	Retrieve data from broadcast	collection	com/adobe/marketing/mobile/LocalNotificationHandler.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/AndroidUlService.java
00012	Read data and put it into a buffer stream	file	com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://amplifon-app-test-emea-edd38.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/601775717631/namespaces/firebase:fetch?key=AlzaSyCms6sj5WJH9Gl9lxZ-iVqrWUuJRO5TD4l. This is indicated by the response: {'state': 'NO_TEMPLATE'}

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	8/44	android.permission.READ_CALENDAR, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, 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

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
trace.browser-intake-us5-datadoghq.com	ok	IP: 34.149.66.134 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
rum-http-intake.logs.datadoghq.eu	ok	IP: 34.95.101.191 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.frozenmountain.com	ok	IP: 138.197.63.67 Country: United States of America Region: New Jersey City: Clifton Latitude: 40.858429 Longitude: -74.163757 View: Google Map
logs.browser-intake-datadoghq.com	ok	IP: 3.233.158.26 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
trace.browser-intake-datadoghq.com	ok	IP: 3.233.158.22 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
logs.browser-intake-us5-datadoghq.com	ok	IP: 34.149.66.134 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
www.ietf.org	ok	IP: 104.16.45.99 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
intake.profile.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
rum.browser-intake-us5-datadoghq.com	ok	IP: 34.149.66.134 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
amplifon-app-test-emea-edd38.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
www.youtube.com	ok	IP: 142.250.179.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
service.xirsys.com	ok	IP: 159.65.109.225 Country: United States of America Region: California City: Santa Clara Latitude: 37.354111 Longitude: -121.955238 View: Google Map

DOMAIN	STATUS	GEOLOCATION
rum.browser-intake-datadoghq.com	ok	IP: 3.233.158.31 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
127.0.0.1	ok	IP: 127.0.0.1 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
rum.browser-intake-ddog-gov.com	ok	IP: 3.30.62.96 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
logs.browser-intake-ddog-gov.com	ok	IP: 3.30.62.23 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
mobile-http-intake.logs.datadoghq.eu	ok	IP: 34.120.77.189 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
rum.browser-intake-us3-datadoghq.com	ok	IP: 68.220.41.19 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
s-intake.s	ok	No Geolocation information available.
www.sonova.com	ok	IP: 151.101.130.191 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
logs.browser-intake-us3-datadoghq.com	ok	IP: 68.220.41.20 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
trace.browser-intake-us3-datadoghq.com	ok	IP: 68.220.41.9 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
global.xirsys.net	ok	IP: 159.65.109.225 Country: United States of America Region: California City: Santa Clara Latitude: 37.354111 Longitude: -121.955238 View: Google Map

DOMAIN	STATUS	GEOLOCATION
ciscobinary.openh264.org	ok	IP: 18.238.96.114 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.webrtc.org	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
trace.browser-intake-ddog-gov.com	ok	IP: 3.32.209.185 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
assets.adobedtm.com	ok	IP: 23.32.229.70 Country: United States of America Region: Georgia City: Atlanta Latitude: 33.749001 Longitude: -84.387978 View: Google Map

EMAILS

EMAIL	FILE
sales@frozenmountain.com	fm/liveswitch/License.java



TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

₽ HARDCODED SECRETS

POSSIBLE SECRETS

"google_crash_reporting_api_key" : "AlzaSyCms6sj5WJH9Gl9lxZ-iVqrWUuJRO5TD4l"

"firebase_database_url": "https://amplifon-app-test-emea-edd38.firebaseio.com"

"google_api_key": "AlzaSyCms6sj5WJH9GI9lxZ-iVqrWUuJRO5TD4l"

DB7C2ABF62E35E668076BEAD2088

0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC

POSSIBLE SECRETS

E95E4A5F737059DC60DFC7AD95B3D8139515620F

0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01

2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

74D59FF07F6B413D0EA14B344B20A2DB049B50C3

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

9a04f079-9840-4286-ab92-e65be0885f95

04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7 E819D7A431D7C90EA0E5F

FFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF
3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A
6D709E02FCE1CDF7E2ECC03404CD28342F619172FE96CB98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAFEF130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42
D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E94E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E68382A9076
00A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F998D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A0075E50DD9020BFD64865036C7AA4E677D2C38532A3A2
3BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB388E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00E6992350511E30ABEC1FFF9E3A26
E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E6229C311562A846505DC82DB854
338AE44F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6880D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF6000C8381E425A31D951AE64FD82FC
EC9509D43687FEB69EDDD1CC5E0B8CC3BDF64B10EF86663142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E45504AC78B75822822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB70
99876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDADA9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDE
D2F8ABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFF

c6450ba3-81af-4737-986a-2217480818ae

1E589A8595423412134FAA2DBDEC95C8D8675E58

POSSIBLE SECRETS 04A1455B334DF099DF30FC28A169A467E9E47075A99F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5 A9FB57DBA1EEA9Bc3E660A9099D83BD726E3BF623D52620282013481D1F6E5377 MQWithSHA512KDFAndSharedInfo 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F 04B8266A46C55657AC734CE38F018F2192 F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03 883423532389192164791648750360308885314476597252960362792450860609699839 9cdbd84c9f1ac2f38d0180142ab952e7338blf511 115792089210356248762697446949407573529996955224135760342422259061068512044369 E101217D4320A90452C760A58EDCD30C8DD06983C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

3045AE6FC8422F64ED579528D38120EAE12196D5

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FA
AAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A277
5D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

POSSIBLE SECRETS
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
SchemasMobileSdkHealthIntervalLoggingEnergyExpenditureTable010
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
07A526C63D3E25A256A007699F5447E32AE456B50E
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
0307AF69989546103D79329FCC3D74880F33BBE803CB
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
3045AE6FC8422f64ED579528D38120EAE12196D5
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
48facb60-c0d9-11e5-b34c-0002a5d5c51b
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7

POSSIBLE SECRETS FFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551 fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17 0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8 00F50B028E4D696E676875615175290472783FB1 fffffff00000000ffffffffffffbce6faada7179e84f3b9cac2fc632551 678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4 0ae0669a-9d66-4cf2-94e9-a46f134b4b07 B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC 9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF 1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C 0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287 662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04 B4E134D3FB59EB8BAB57274904664D5AF50388BA 02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7 040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883 42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797 452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1 b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a 2AA058F73A0E33AB486B0F610410C53A7F132310 4099B5A457F9D69F79213D094C4BCD4D4262210B 040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150 91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28

fswSlashFittingLogSlashHearingDeviceOptionsSlashVolumeControlSlash0Period1Period0

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
7d7374168ffe3471b60a857686a19475d3bfa2ff
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
6db14acc9e21c820ff28b1d5ef5de2b0
985BD3ADBAD4D696E676875615175A21B43A97E3
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
3086d221a7d46bcde86c90e49284eb15
b8adf1378a6eb73409fa6c9c637ba7f5
9760508f15230bccb292b982a2eb840bf0581cf5
AADD9D88DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
010092537397ECA4F6145799D62B0A19CE06FE26AD
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
E95E4A5F737059DC60DF5991D45029409E60FC09
10E723AB14D696E6768756151756FEBF8FCB49A9
fswSlashFittingLogSlashHearingDeviceOptionsSlashVolumeQuickSyncSlash0Period1Period0
fswSlashFittingLogSlashHearingDeviceOptionsSlashAcousticAcknowledgmentSlash0Period1Period0
9BA05972-F6A8-11CF-A442-00A0C90A8F39
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E46462177918 11142820341263C5315

POSSIBLE SECRETS
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
6b8cf07d4ca75c88957d9d670591
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
3086d221a7d46bcde86c90e49284eb153dab
3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
SchemasMobileSdkFirmwareUpdateFirmwareUpdateProcess010NonRechargeableBatteryInfo
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
4D696E676875615175985BD3ADBADA21B43A97E2
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
e3f1f98c9da02a93bb547f448b472d727e14b22455235796fe49863856252508
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
020A601907B8C953CA1481EB10512F78744A3205FD
c06c8400-8e06-11e0-9cb6-0002a5d5c51b

POSSIBLE SECRETS

1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD

32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE6
4B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F157
5A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

71169be7330b3038edb025f1

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFC
B5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F32937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFA
D1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2
F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A2979
9620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259

EA1AFB91-9E28-4B86-90E9-9E9F8A5EEFAF

00E8BEE4D3E2260744188BE0E9C723

 $13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331056774413619636480306472137782665689868646846\\3277710150809401182608770201615324990468332931294920912776241137878030224355746606283971659376426832674269780880061631528163475887$

B99B99B099B323E02709A4D696E6768756151751

f21d7497-b7ec-4340-b5f6-f2941de930cf

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF704
20EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB
66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C
1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055
AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B

5181942b9ebc31ce68dacb56c16fd79f

POSSIBLE SECRETS
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
fswFittingLogFittingSideProgramResponseDisplayCurvesV2010
79885141663410976897627118935756323747307951916507639758300472692338873533959
90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614 056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065
D6031998D1B3BBFEBF59CC9BBFF9AEE1
b3fb3400dec5c4adceb8655d4c94
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
24B7B137C8A14D696E6768756151756FD0DA2E5C
ae2044fb577e65ee8bb576ca48a2f06e
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
10B7B4D696E676875615175137C8A16FD0DA2211
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
03F7061798EB99E238FD6F1BF95B48FEEB4854252B

POSSIBLE SECRETS
6b8cf07d4ca75c88957d9d67059037a4
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
962eddcc369cba8ebb260ee6b6a126d9346e38c5
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
401028774D7777C7B7666D1366EA432071274F89FF01E718
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A 57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
6ba7b810-9dad-11d1-80b4-00c04fd430c8
db92371d2126e9700324977504e8c90e
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
659EF8BA043916EEDE8911702B22
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

POSSIBLE SECRETS
03E5A88919D7CAFCBF415F07C2176573B2
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BC A95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
D2C0FB15760860DEF1EEF4D696E6768756151754
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
MQVwithSHA256KDFAndSharedInfo
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F5051525354555657 58595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAE AFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
546015050999c60f542e0ccc80ae5abf
CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
5c4ece41241a1bb513f6e3e5df74ab7d5183dfffbd71bfd43127920d880569fd
41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67
85E25BFE5C86226CDB12016F7553F9D0E693A268
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE

POSSIBLE SECRETS
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
85CB6900-4D95-11CF-960C-0080C7F4EE85
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
D09E8800291CB85396CC6717393284AAA0DA64BA
fswFittingLogHearingDeviceOptionsVolumeQuickSync010
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
8d5155894229d5e689ee01e6018a237e2cae64cd
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
e43bb460f0b80cc0c0b075798e948060f8321b7d
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
80480cda-ebcf-4c2f-b48b-b8eccda805b6
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC 2B2912675BF5B9E582928
C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE428782A95ECA1C143DB701FD48533A3C18F0FE23557EA 7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562CE1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DB C2D364AADE99BE0D0AAD82E5320121496DC65B3930E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd

POSSIBLE SECRETS

517cc1b727220a94fe13abe8fa9a6ee0

7A1F6653786A68192803910A3D30B2A2018B21CD54

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

 $fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a615\\0f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7$

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8 096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520 086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

SchemasFswFittingLogFittingSideProgramResponseDisplayCurvesV2010

0217C05610884B63B9C6C7291678F9D341

6C01074756099122221056911C77D77E77A777E7E7E7F7FCB

021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F

115792089210356248762697446949407573530086143415290314195533631308867097853951

SchemasMobileSdkHealthIntervalLoggingStepCountTable010

04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

4A6E0856526436F2F88DD07A341E32D04184572BEB710

03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a

7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE

POSSIBLE SECRETS
7fffffffffffffffffffffffffffffffffffff
C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346 d3f529252
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
0340340340340340340340340340340340340340
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB7 3D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63
0095E9A9EC9B297BD4BF36E059184F
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72

POSSIBLE SECRETS EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF 1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3 0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D 9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D7598 9B9F605F5A858107AB1EC85E6B41C8AA582CA3511EDDFB74F02F3A6598980BB9 91771529896554605945588149018382750217296858393520724172743325725474374979801 96341f1138933bc2f503fd44 1524625445295769349356752728956831541775441763139384457191755096847107846595662547942312293338483924514339614727760681880609734239 A335926AA319A27A1D00896A6773A4827ACDAC73 1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10 0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500 6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a c469684435deb378c4b65ca9591e2a5763059a2e 340E7BE2A280EB74E2BE61BADA745D97E8F7C300 68363196144955700784444165611827252895102170888761442055095051287550314083023 7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E 0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205 040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6 C42E9C55215AA9CA27A5863EC48D8E0286B 000E0D4D696E6768756151750CC03A4473D03679 470fa2b4ae81cd56ecbcda9735803434cec591fa

POSSIBLE SECRETS F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F 7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA 3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1 2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE 6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF 42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778114ca50f7a8e2f3f657c1108d9d44cfd8 04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886 DB7C2ABF62E35E7628DFAC6561C5 07A11B09A76B562144418FF3FF8C2570B8 1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F MQVwithSHA384KDFAndSharedInfo 072546B5435234A422E0789675F432C89435DE5242 047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44 E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148 fswSlashFittingLogSlashFittingSideProgramSlashResponseDisplayCurvesV2Slash0Period1Period00432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0 22123dc2395a05caa7423daeccc94760a7d462256bd56916 9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BA B63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2 442C6F315180F93499A234DCF76E3FED135F9BB

POSSIBLE SECRETS
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
SchemasMobileSdkHealthIntervalLoggingActivityTimeTable010
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B7 1634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
DB7C2ABF62E35E668076BEAD208B
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
12511cfe811d0f4e6bc688b4d
92139cd3409b652be06d98104929f9b2
002757A1114D696E6768756151755316C05E0BD4
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
10099790675505530477208181553592522486984108257205345787482351587557714799052927277724415285269929879648335669968284202797289605274717317548059048560713474685214192868091256150280 2222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588322876850946740663962
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
31a92ee2029fd10d901b113e990710f0d21ac6b6

POSSIBLE SECRETS
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
127971af8721782ecffa3
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
7B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
51DEF1815DB5ED74FCC34C85D709
b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046
1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de
5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1

POSSIBLE SECRETS
5FF6108462A2DC8210AB403925E638A19C1455D21
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
003088250CA6E7C7FE649CE85820F7
FFFFFFE0000000075A30D1B9038A115
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
5EEEFCA380D02919DC2C6558BB6D8A5D
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
SchemasHSResultsMonaural4TonesWithAudiogramPrediction010
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F385 14F1FDF4B4F40D2181B3681C364BA0273C706
5F49EB26781C0EC6B8909156D98ED435E45FD59918
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
c49d360886e704936a6678e1139d26b7819f7e90

POSSIBLE SECRETS
71169be7330b3038edb025f1d0f9
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
37c33cdd-a5ac-41cf-90c1-5834818082e2
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
1243ae1b4d71613bc9f780a03690e
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
SchemasMobileSdkHealthUsagePeriodUnixTimeOfBootTable010
6EE3CEEB230811759F20518A0930F1A4315A827DAC
9162fbe73984472a0a9d0590
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A

POSSIBLE SECRETS
004D696E67687561517512D8F03431FCE63B88F4
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb6 27a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
e8b4011604095303ca3b8099982be09fcb9ae616
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F5 4449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
6127C24C05F38A0AAAF65C0EF02C
56FDF344-FD6D-11d0-958A-006097C9A090
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
4E13CA542744D696E67687561517552F279A8C84
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

POSSIBLE SECRETS
SchemasFswFittingLogHearingDeviceOptionsVolumeQuickSync010
10C0FB15760860DEF1EEF4D696E676875615175D
103FAEC74D696E676875615175777FC5B191EF30
c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
1053CDE42C14D696E67687561517533BF3F83345
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
C49D360886E704936A6678E1139D26B7819F7E90
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
56FDF342-FD6D-11D0-958A-006097C9A090
e4437ed6010e88286f547fa90abfe4c42212
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0108B39E77C4B108BED981ED0E890E117C511CF072
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D

POSSIBLE SECRETS e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab 127a3daf 0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1 E87579C11079F43DD824993C2CEE5ED3 36DF0AAFD8B8D7597CA10520D04B 12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499672425412104927434935707492031276956145168922 139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803187341288580489525163 00689918DBEC7E5A0DD6DFC0AA55C7 036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773 8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14 6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40 A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353 04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3 60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788 1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45 2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988 E95E4A5F737059DC60DFC7AD95B3D8139515620C 617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c 0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521

POSSIBLE SECRETS

FFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6
B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F3556208552BB9ED529077096966D670C354E4ABC
9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF
1CBA64ECFB850458DBEF00A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A225619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C
0BA0946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD444CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287
C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646
DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B323051512BD7AF426FB8F401378CD2BF5983CA01C6
4B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A884031900B1C9E59E7C97FBEC7E8F323A97A7E36C88BE0F1D458F7F585AC54BD407BB22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EE
F29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C046804328F663F4860EE12BF2D580B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8C2BEC4
D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F56834238F442BF1C978238F16CBE39D652DE3FDB8BFC848AD922222E04A44037C0713EB57A81A23F0C73473FC646CEA306B4BC
BC8862F8388DDFA904B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F4448EDDF310EE074AB6A364597E899A0255DC164F31CC50846851D99AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA26
8359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9A9E3050E2765694DFC81F56E880B96E7160C980DD98EDDJ3DF

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53

4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

∷ SCAN LOGS

Timestamp	Event	Error
2025-08-31 05:15:39	Generating Hashes	ОК
2025-08-31 05:15:39	Extracting APK	OK
2025-08-31 05:15:39	Unzipping	ОК
2025-08-31 05:15:40	Parsing APK with androguard	ОК
2025-08-31 05:15:40	Extracting APK features using aapt/aapt2	ОК

2025-08-31 05:15:41	Getting Hardcoded Certificates/Keystores	ОК
2025-08-31 05:15:43	Parsing AndroidManifest.xml	OK
2025-08-31 05:15:43	Extracting Manifest Data	OK
2025-08-31 05:15:43	Manifest Analysis Started	OK
2025-08-31 05:15:43	Performing Static Analysis on: Miracle-Ear (com.miracleear.mdapp)	OK
2025-08-31 05:15:55	Fetching Details from Play Store: com.miracleear.mdapp	OK
2025-08-31 05:15:56	Checking for Malware Permissions	OK
2025-08-31 05:15:56	Fetching icon path	OK
2025-08-31 05:15:56	Library Binary Analysis Started	OK
2025-08-31 05:15:56	Analyzing ddtrot/jni/sparcv9-SunOS/libjffi- 1.2.so	OK
2025-08-31 05:15:56	Analyzing ddtrot/jni/x86_64-SunOS/libjffi- 1.2.so	ОК
2025-08-31 05:15:56	Analyzing ddtrot/jni/sparcv9-Linux/libjffi- 1.2.so	OK
2025-08-31 05:15:56	Analyzing ddtrot/jni/x86_64- FreeBSD/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing ddtrot/jni/x86_64- DragonFlyBSD/libjffi-1.2.so	OK

2025-08-31 05:15:56	Analyzing ddtrot/jni/mips64el-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/x86_64-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/i386-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/x86_64- OpenBSD/libjffi-1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/s390x-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/aarch64-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/arm-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/i386-SunOS/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing ddtrot/jni/aarch64- FreeBSD/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing ddtrot/jni/ppc64-Linux/libjffi- 1.2.so	ОК
2025-08-31 05:15:56	Analyzing ddtrot/jni/ppc64le-Linux/libjffi- 1.2.so	ок
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/sparcv9- SunOS/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/x86_64- SunOS/libjffi-1.2.so	ОК

2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/sparcv9- Linux/libjffi-1.2.so	ок
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/x86_64- FreeBSD/libjffi-1.2.so	ок
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/x86_64- DragonFlyBSD/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/mips64el- Linux/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/x86_64- Linux/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/i386- Linux/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/x86_64- OpenBSD/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/s390x- Linux/libjffi-1.2.so	OK
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/aarch64- Linux/libjffi-1.2.so	OK
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/arm- Linux/libjffi-1.2.so	OK
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/i386- SunOS/libjffi-1.2.so	ОК
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/aarch64- FreeBSD/libjffi-1.2.so	ОК

2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/ppc64- Linux/libjffi-1.2.so	OK
2025-08-31 05:15:56	Analyzing apktool_out/unknown/ddtrot/jni/ppc64le- Linux/libjffi-1.2.so	OK
2025-08-31 05:15:56	Reading Code Signing Certificate	OK
2025-08-31 05:15:57	Running APKiD 2.1.5	OK
2025-08-31 05:16:09	Detecting Trackers	OK
2025-08-31 05:16:17	Decompiling APK to Java with JADX	OK
2025-08-31 05:26:15	Decompiling with JADX failed, attempting on all DEX files	ОК
2025-08-31 05:26:15	Decompiling classes6.dex with JADX	OK
2025-08-31 05:26:28	Decompiling classes2.dex with JADX	OK
2025-08-31 05:26:40	Decompiling classes4.dex with JADX	ОК
2025-08-31 05:26:59	Decompiling classes.dex with JADX	ОК
2025-08-31 05:27:10	Decompiling classes3.dex with JADX	OK
2025-08-31 05:27:21	Decompiling classes5.dex with JADX	ОК

2025-08-31 05:27:32	Decompiling classes7.dex with JADX	ок
2025-08-31 05:27:36	Decompiling classes6.dex with JADX	ОК
2025-08-31 05:27:49	Decompiling classes2.dex with JADX	ок
2025-08-31 05:28:01	Decompiling classes4.dex with JADX	ок
2025-08-31 05:55:02	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/b3a15512ad7994dc9e4a1a53eb68c3a7/java_source', '-q', '-r', 'show-bad-code', '/home/mobsf/.MobSF/uploads/b3a15512ad7994dc9e4a1a53eb68c3a7/apktool_out/classes4.dex'], 999.9999840259552)
2025-08-31 05:55:02	Converting DEX to Smali	ок
2025-08-31 05:55:02	Code Analysis Started on - java_source	ок
2025-08-31 05:55:46	Android SBOM Analysis Completed	ок
2025-08-31 05:56:03	Android SAST Completed	ок
2025-08-31 05:56:03	Android API Analysis Started	ок
2025-08-31 05:56:22	Android API Analysis Completed	ок
2025-08-31 05:56:22	Android Permission Mapping Started	ок
2025-08-31 05:56:42	Android Permission Mapping Completed	ок
2025-08-31 05:56:44	Android Behaviour Analysis Started	ОК

2025-08-31 05:57:01	Android Behaviour Analysis Completed	ок
2025-08-31 05:57:01	Extracting Emails and URLs from Source Code	ОК
2025-08-31 05:57:19	Email and URL Extraction Completed	ОК
2025-08-31 05:57:19	Extracting String data from APK	ок
2025-08-31 05:57:19	Extracting String data from SO	ок
2025-08-31 05:57:19	Extracting String data from Code	ОК
2025-08-31 05:57:19	Extracting String values and entropies from Code	ок
2025-08-31 06:18:46	Performing Malware check on extracted domains	ок
2025-08-31 06:18:53	Saving to Database	ОК

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.