MOBSF

ANDROID STATIC ANALYSIS REPORT

Oregon ONE Mobile (2.0.14)

File Name:	gov.or.oregonone_5439001.apk
Package Name:	gov.or.oregonone
Scan Date:	Sept. 1, 2025, 1:25 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	12	3	1	1

FILE INFORMATION

File Name: gov.or.oregonone_5439001.apk
Size: 27.67MB
MD5: b788921d8f5ee4f2e9ed3756381540f2
SHA1: 657267fa5a50084b500c7879104ac849d0fbd9de
SHA256: bad53819f821217ba5a7a0ce447ef0cfcb99af0bcfa4d8f34a3e6e6be8206118

APP INFORMATION

App Name: Oregon ONE Mobile
Package Name: gov.or.oregonone
Main Activity: gov.or.oregonone.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.0.14

Android Version Code: 5439001

APP COMPONENTS

Activities: 21
Services: 6
Receivers: 4
Providers: 5
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-03-09 08:48:28+00:00
Valid To: 2053-03-09 08:48:28+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf03358026716cef8778444ca7f25965eb9cdf9fb
Hash Algorithm: sha256
md5: 5b1ca1c0a88e728d0b175dd85fb1017d
sha1: 977f2d9ef2ea221d3ba25ac2efc3a9fffa9ef349
sha256: a74e49baeabcf8410f72b5509706e08627bf77684c529fef906b5997addeeb30
sha512: 9067ca059c568dbea2653ea91cae57d81d1afe07e2b0e922df9eeab02549c8e9050ebaf7a562cdaf97c4ce2a9d8b55a4d2ab7582938ef978034fca48d76f4a7c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 0374bf875f6f37893eccaa2e4270167887da80a00cce7c7981ec93f95de9c5ac
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
gov.or.oregonone.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
b788921d8f5ee4f2e9ed3756381540f2.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 3 | 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. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (gov.or.oregonone.CaptureActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	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.

CODE ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 3 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/ammarahmed/mmkv/RNMMKVModule.java com/ammarahmed/mmkv/SecureKeystore.java com/dieam/reactnativepushnotification/helpers/ApplicationBadgeHelper.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modules/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPicturesAggregator.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modules/RNReceivedMessageHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dles/RNReceivedMessageHandler.java com/github/bartekSC/pdfviewer/PDFView.java com/github/bartekSC/pdfviewer/RenderingHandler.java com/github/bartekSC/pdfviewer/link/DefaultLinkHandler.java com/henninghall/date_picker/DerivedData.java com/henninghall/date_picker/pickers/AndroidNative.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/kofax/kmc/ken/engines/ImageProcessor.java com/kofax/kmc/kut/utilities/Sizeof.java com/kofax/kmc/kut/utilities/appstats/AppStatsNewJsonExportHandler.java com/kofax/mobile/sdk/aj/a.java com/kofax/mobile/sdk/m/a.java com/kofax/mobile/sdk/m/d.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/Flags.java com/microsoft/appcenter/ServiceInstrumentation.Utils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ationUtils.java com/microsoft/appcenter/UncaughtExceptionHandler.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/AnalyticsTransmissionTarget.java com/microsoft/appcenter/analytics/AuthenticationProvider.java com/microsoft/appcenter/analytics/EventProperties.java com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java com/microsoft/appcenter/analytics/channel/SessionTracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/channel/OneCollectorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java com/microsoft/appcenter/http/DefaultHttpClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/microsoft/appcenter/http/DefaultHttpClientCallTask.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/reactnative/analytics/AppCenterReactNativeAnalyticsModule.java com/microsoft/appcenter/reactnative/appcenter/AppCenterReactNativeModule.java com/microsoft/appcenter/reactnative/appcenter/ReactNativeUtils.java com/microsoft/appcenter/reactnative/crashes/AppCenterReactNativeCrashesUtils.java com/microsoft/appcenter/reactnative/shared/AppCenterReactNativeShared.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java com/microsoft/appcenter/utils/NetworkStateHelper.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/context/UserIdContext.java com/microsoft/appcenter/utils/crypto/Crypt

NO	ISSUE	SEVERITY	STANDARDS	FILES
				oUtils.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/appcenter/utils/storage/FileManager.java com/microsoft/windowsazure/messaging/notificationhubs/NetworkStateHelper.java com/microsoft/windowsazure/messaging/notificationhubs/NotificationHub.java com/microsoft/windowsazure/messaging/notificationhubs/NotificationHubExtension.java com/reactcommunity/rndatetimepicker/Common.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnbootsplash/RNBootSplashModuleImpl.java com/zoontek/rnpermissions/RNPermissionsModuleImpl.java gov/or/oregonone/CaptureActivity.java io/legere/pdfiumandroid/DefaultLogger.java io/legere/pdfiumandroid/PdfiumCore.java me/leolin/shortcutbadger/ShortcutBadger.java net/time4j/android/ApplicationStarter.java net/time4j/base/ResourceLoader.java net/time4j/format/expert/ChronoFormatter.java net/time4j/format/expert/CustomizedProcessor.java net/time4j/format/expert/DecimalProcessor.java net/time4j/format/expert/FormatStep.java net/time4j/format/expert/FractionProcessor.java net/time4j/format/expert/IgnorableWhitespaceProcessor.java net/time4j/format/expert/Iso8601Format.java net/time4j/format/expert/LiteralProcessor.java net/time4j/format/expert/LocalizedGMTProcessor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/time4j/format/expert/LookupProcessor.java net/time4j/format/expert/MultiFormatParser.java net/time4j/format/expert/NumberProcessor.java net/time4j/format/expert/OrdinalProcessor.java net/time4j/format/expert/SkipProcessor.java net/time4j/format/expert/StyleProcessor.java net/time4j/format/expert/TextProcessor.java net/time4j/format/expert/TimezoneGenericProcessor.java net/time4j/format/expert/TimezoneIDProcessor.java net/time4j/format/expert/TimezoneNameProcessor.java net/time4j/format/expert/TimezoneOffsetProcessor.java net/time4j/format/expert/TwoDigitYearProcessor.java net/time4j/i18n/WeekdataProviderSPI.java net/time4j/tz/spi/ZoneNameProviderSPI.java org/kobjects/repackaged/crypt/Crypt.java org/kobjects/repackaged/mime/Decoder.java org/kobjects/repackaged/pim/PimParser.java org/kxml2/repackaged/io/KXmlParser.java org/wonday/pdf/PdfView.java org/xmlpull/repackaged/v1/XmlPullParserException.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/kofax/kmc/ken/engines/ocr/OcrEngine.java com/kofax/kmc/ken/engines/service/FileService.java com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java com/kofax/kmc/kut/utilities/appstats/AppStatsMsSqlExportHandler.java com/kofax/mobile/sdk/_internal/impl/camera/aj.java com/kofax/mobile/sdk/aj/a.java com/kofax/mobile/sdk/w/c.java com/kofax/mobile/sdk/w/d.java com/learnium/RNDeviceInfo/RNDeviceModule.java
3	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/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/kofax/mobile/sdk/extract/id/LocalProjectProvider.java com/kofax/mobile/sdk/extract/id/bundle/ZipFileBundle.java com/kofax/mobile/sdk/extract/id/bundle/ZipInputStreamBundle.java
				com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/kofax/mobile/sdk/_internal/impl/extraction/kta/KtaServiceCaller.java com/kofax/mobile/sdk/_internal/impl/extrac

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tion/kta/kmd/g.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/reactnative/appcenter/ReactNativeUtils.java com/microsoft/appcenter/reactnative/shared/AppCenterReactNativeShared.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/windowsazure/messaging/Connection.java com/microsoft/windowsazure/messaging/NotificationHub.java com/microsoft/windowsazure/messaging/notificationhubs/ConnectionString.java com/microsoft/windowsazure/messaging/notificationhubs/DebounceInstallationAdapter.java com/microsoft/windowsazure/messaging/notificationhubs/IdAssignmentVisitor.java com/microsoft/windowsazure/messaging/notificationhubs/NotificationHub.java com/microsoft/windowsazure/messaging/notificationhubs/PlatformVisitor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/windowsazure/messaging/notificationhubs/PushChannelVisitor.java com/microsoft/windowsazure/messaging/notificationhubs/TagVisitor.java com/microsoft/windowsazure/messaging/notificationhubs/TemplateVisitor.java com/microsoft/windowsazure/messaging/notificationhubs/UserIdVisitor.java
5	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	net/time4j/tz/spi/WinZoneProviderSPI.java com/ReactNativeBlobUtil/ReactNativeBlobUtilUtils.java com/airbnb/lottie/network/NetworkCache.java okio/repackaged/Buffer.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/kofax/BuildConfig.java com/kofax/kmc/ken/engines/data/Image.java com/kofax/kmc/ken/engines/data/ImagePerfectionProfile.java com/kofax/kmc/ken/engines/data/QuickAnalysisFeedback.java com/kofax/kmc/ken/engines/version/KenVersion.java com/kofax/kmc/klo/logistics/data/DocumentType.java com/kofax/kmc/klo/logistics/version/KloVersion.java com/kofax/kmc/kui/uicontrols/version/KuiVersion.java com/kofax/kmc/kut/utilities/SdkVersion.java com/kofax/kmc/kut/utilities/version/KutVersion.java
7	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
9	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/kofax/kmc/kut/utilities/appstats/AppStatsSqLiteDs.java
10	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/microsoft/appcenter/http/HttpClientRetryer.java org/kobjects/repackaged/crypt/Crypt.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/ReactNativeBlobUtil/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00036	Get resource file from res/raw directory	reflection	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/microsoft/appcenter/utils/DeviceInfoHelper.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/kofax/kmc/klo/logistics/service/NetworkService.java com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/kofax/kmc/klo/logistics/service/NetworkService.java com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/microsoft/windowsazure/messaging/Connection.java org/ksoap2/repackaged/transport/ServiceConnectionSE.java
00089	Connect to a URL and receive input stream from the server	command network	com/microsoft/windowsazure/messaging/Connection.java org/ksoap2/repackaged/transport/ServiceConnectionSE.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/microsoft/windowsazure/messaging/Connection.java org/ksoap2/repackaged/transport/ServiceConnectionSE.java
00109	Connect to a URL and get the response code	network command	com/microsoft/windowsazure/messaging/Connection.java org/ksoap2/repackaged/transport/ServiceConnectionSE.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilMediaCollection.java com/ReactNativeBlobUtil/ReactNativeBlobUtilStream.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/ammarahmed/mmkv/Storage.java com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java com/kofax/mobile/sdk/_internal/impl/camera/n.java com/kofax/mobile/sdk/_internal/impl/extraction/onDevice/ep.java com/kofax/mobile/sdk/_internal/impl/extraction/onDevice/l.java com/kofax/mobile/sdk/extract/id/LocalProjectProvider.java com/kofax/mobile/sdk/extract/id/ServerProjectProvider.java com/kofax/mobile/sdk/l/d.java com/microsoft/appcenter/utils/storage/FileManager.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java okio/Okio__JvmOkioKt.java okio/repackaged/Okio.java org/ksoap2/repackaged/transport/HttpTransportSE.java
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/airbnb/lottie/LottieCompositionFactory.java
00002	Open the camera and take picture	camera	com/kofax/mobile/sdk/_internal/impl/camera/ad.java com/kofax/mobile/sdk/_internal/impl/camera/p.java
00183	Get current camera parameters and change the setting.	camera	com/kofax/mobile/sdk/_internal/impl/camera/ad.java com/kofax/mobile/sdk/_internal/impl/camera/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ReactNativeBlobUtil/ReactNativeBlobUtilImpl.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/github/bartekscpdfviewer/link/DefaultLinkHandler.java com/vinzscam/reactnativefileviewer/RNFileViewerModule.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/kofax/kmc/ken/engines/ImageProcessor.java com/kofax/kmc/ken/engines/data/Image.java com/kofax/kmc/ken/engines/ocr/OcrEngine.java com/kofax/kmc/ken/engines/service/FileService.java com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java com/kofax/mobile/sdk/_internal/impl/camera/ad.java com/kofax/mobile/sdk/_internal/impl/camera/aj.java com/kofax/mobile/sdk/_internal/impl/camera/ao.java com/kofax/mobile/sdk/_internal/impl/camera/n.java com/kofax/mobile/sdk/_internal/impl/extraction/onDevice/l.java com/kofax/mobile/sdk/aj/a.java com/kofax/mobile/sdk/extract/id/LocalProjectProvider.java com/kofax/mobile/sdk/extract/id/bundle/BundleCacheProvider.java com/kofax/mobile/sdk/k/c.java com/kofax/mobile/sdk/l/d.java com/kofax/mobile/sdk/logistics/CaptureServer.java com/kofax/mobile/sdk/p/a.java com/kofax/mobile/sdk/w/c.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java com/reactnativedocumentpicker/RNDocumentPickerModule.java gov/or/oregonone/CaptureActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00014	Read file into a stream and put it into a JSON object	file	com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/kmc/kui/uicontrols/ImageService.java
00123	Save the response to JSON after connecting to the remote server	network command	com/kofax/kmc/kui/uicontrols/ImageService.java
00192	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java com/kofax/kmc/ken/engines/service/FileService.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java
00094	Connect to a URL and read data from it	command network	net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/kofax/kmc/ken/engines/service/ImageService.java com/kofax/mobile/sdk/an/a.java
00175	Get notification manager and cancel notifications	notification	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00012	Read data and put it into a buffer stream	file	org/ksoap2/repackaged/transport/HttpTransportSE.java
00195	Set the output path of the recorded file	record file	com/kofax/mobile/sdk/_internal/impl/camera/ad.java
00199	Stop recording and release recording resources	record	com/kofax/mobile/sdk/_internal/impl/camera/ad.java
00198	Initialize the recorder and start recording	record	com/kofax/mobile/sdk/_internal/impl/camera/ad.java
00007	Use absolute path of directory for the output media file path	file	com/kofax/mobile/sdk/_internal/impl/camera/ad.java
00196	Set the recorded file format and output path	record file	com/kofax/mobile/sdk/_internal/impl/camera/ad.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	com/kofax/kmc/ken/engines/service/ImageService.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/829911294159/namespaces/firebase:fetch?key=AIzaSyBvvk_YWMz0FIxLXKHenyF42g1hRulLQJM. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	2/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
util.wsc.des.kofax.com	ok	No Geolocation information available.
login.wsc.des.kofax.com	ok	No Geolocation information available.
indexfields.wsc.des.kofax.com	ok	No Geolocation information available.
mobile.events.data.microsoft.com	ok	**IP:** 20.42.73.26 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
profile.wsc.des.kofax.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.xmlsoap.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scansettings.wsc.des.kofax.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
device.wsc.des.kofax.com	ok	No Geolocation information available.
job.wsc.des.kofax.com	ok	No Geolocation information available.
wsc.des.kofax.com	ok	No Geolocation information available.
www.wireless-village.org	ok	**IP:** 104.21.11.240 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xml.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
in.appcenter.ms	ok	**IP:** 20.57.103.21 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
logout.wsc.des.kofax.com	ok	No Geolocation information available.
www.openmobilealliance.org	ok	**IP:** 104.26.8.105 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_preference_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.FirebasePreferences"
"google_api_key" : "AIzaSyBvvk_YWMz0FIxLXKHenyF42g1hRulLQJM"
"google_crash_reporting_api_key" : "AIzaSyBvvk_YWMz0FIxLXKHenyF42g1hRulLQJM"
"installation_enrichment_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.InstallationSharedPreferences"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
8C261B3A-125D-4EC2-990D-33AA824A6890
5C62C3BE32CA208BD81CAE8F4390CEA5B3E36DD5BCA6379291B4A0F398A5F437

POSSIBLE SECRETS
076F86B485C8E77B90FC504C5CBE62C710B1D4EACB687C4211B688AE073E85A0
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
e4b001df9a082298dd090bb7455c45d92fbd5dda
CA10BF68-FD0D-4217-AF1D-8A0711ED39D7
5C6F013332805C58FA52848F854B6DD4B593CE2A91AF0CAAE252E0D8C50B9A9B
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
5C44241E3E38A6E3BFBA3FB5949112DA91544173A67BFA58B622123B0C5341BC
2CA472C41CEF35CFDC61211A06C1AEF49AD8D4405B07598C6008F4287D34ACFA
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
5A52C54FD2EEB8A9DC6599740ABB69E6B397378ADBE1CE342517D4700C9F56AD
2DBAB7E1F20796746AFA20069DE9F5B7C2D5CAA2F63A86BB6B89634D6C4336DD
722D1BF70863DBF0D933606DC43A259E2B0DFE7BE1DEAF3F7A5599CEBF076BC3
295D23C3BCCF2A8C4E684BE761DFA13C44F30E15A707430D645BC4584083491B

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
9A5282B31BBFF5DDA1B564105401D219B8C5A5832EE7897D42E2B1C83F487B59
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
01360240043788015936020505
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

PLAYSTORE INFORMATION

Title: Oregon ONE Mobile

Score: 3.43 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** gov.or.oregonone

Developer Details: OHA - ODHS, OHA+-+ODHS, None, https://www.oregon.gov/dhs, ONE.Infrastructure@dhsoha.state.or.us,

Release Date: Apr 21, 2023 **Privacy Policy:** Privacy link

Description:

Oregon ONE Mobile is an official State of Oregon app. You can securely mange and take steps to apply for public medical, food, cash and child care. You don’t always have to call, go into an office or find a desktop computer. You can do a lot from your smartphone. Try it out. Available in English and Spanish. • See if your case or application is approved, denied, pending, closed and what actions you need to take. • See and download notices that were mailed to you • Check out your next renewal/periodic report due date, for SNAP, CASH, ERDC, and Medical Assistance. • Get important, time-sensitive alerts and notifications about your benefits. • Take pictures of supporting documents and attach them to get benefits. • Manage your ONE Online account email and password • Find a guided tour of the app, FAQs, and referrals for additional resources. You must have an existing ONE Online account. No costs except for data rates.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:25:44	Generating Hashes	OK
2025-09-01 13:25:44	Extracting APK	OK
2025-09-01 13:25:44	Unzipping	OK
2025-09-01 13:25:44	Parsing APK with androguard	OK
2025-09-01 13:25:44	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:25:45	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:25:47	Parsing AndroidManifest.xml	OK

2025-09-01 13:25:47	Extracting Manifest Data	OK
2025-09-01 13:25:47	Manifest Analysis Started	OK
2025-09-01 13:25:47	Performing Static Analysis on: Oregon ONE Mobile (gov.or.oregonone)	OK
2025-09-01 13:25:48	Fetching Details from Play Store: gov.or.oregonone	OK
2025-09-01 13:25:50	Checking for Malware Permissions	OK
2025-09-01 13:25:50	Fetching icon path	OK
2025-09-01 13:25:50	Library Binary Analysis Started	OK
2025-09-01 13:25:50	Reading Code Signing Certificate	OK
2025-09-01 13:25:50	Running APKiD 2.1.5	OK
2025-09-01 13:25:55	Detecting Trackers	OK

2025-09-01 13:25:58	Decompiling APK to Java with JADX	OK
2025-09-01 13:26:15	Converting DEX to Smali	OK
2025-09-01 13:26:15	Code Analysis Started on - java_source	OK
2025-09-01 13:26:17	Android SBOM Analysis Completed	OK
2025-09-01 13:26:26	Android SAST Completed	OK
2025-09-01 13:26:26	Android API Analysis Started	OK
2025-09-01 13:26:33	Android API Analysis Completed	OK
2025-09-01 13:26:33	Android Permission Mapping Started	OK
2025-09-01 13:26:40	Android Permission Mapping Completed	OK
2025-09-01 13:26:40	Android Behaviour Analysis Started	OK

2025-09-01 13:26:48	Android Behaviour Analysis Completed	OK
2025-09-01 13:26:48	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:26:50	Email and URL Extraction Completed	OK
2025-09-01 13:26:50	Extracting String data from APK	OK
2025-09-01 13:26:50	Extracting String data from Code	OK
2025-09-01 13:26:50	Extracting String values and entropies from Code	OK
2025-09-01 13:26:53	Performing Malware check on extracted domains	OK
2025-09-01 13:26:55	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.