ANDROID STATIC ANALYSIS REPORT

NYSOH Upload (2.4)

File Name:	com.maximus.missinginformation.nysoh_34.apk
Package Name:	com.maximus.missinginformation.nysoh
Scan Date:	Aug. 31, 2025, 2:35 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

◔ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
2	12	1	3	2

📦 FILE INFORMATION

File Name: com.maximus.missinginformation.nysoh_34.apk
Size: 14.64MB
MD5: dfbea3b522637051f752d6f9fe123238
SHA1: e992ef934d1b00ae3c31502316805c1336857ccd
SHA256: c6df94064d79cfd06294a3b12e4ac740b6ef5ddd75ac75a7c7dbc646f41545a9

ℹ APP INFORMATION

App Name: NYSOH Upload
Package Name: com.maximus.missinginformation.nysoh
Main Activity: com.maximus.missinginformation.ui.activities.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.4

Android Version Code: 34

■■ APP COMPONENTS

Activities: 10
Services: 7
Receivers: 3
Providers: 3
Exported Activities: 0
Exported Services: 1
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: 2019-10-10 16:10:21+00:00
Valid To: 2049-10-10 16:10:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc4cfda34ee6412e3bc559afcf5180dbde896a589
Hash Algorithm: sha256
md5: 291579f74bce36b10bda095445e9e991
sha1: ce4f13caa35eca0827e95590f0facb0fc2c198f6
sha256: 526e9ac644871911438802b3ac9e1aadefc771283964c22958f03cae9a7f6de7
sha512: db30babea39990451c3a755ea9d21468cdba5d9438295e2e79f0ce467855a50571378e7cf96e2829e5dd44ba5bf6ac7b7abcb0f8edd16592c0693710bca377ad
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5a66b688a6f4e4783221fe453c5b3ff26221d7637afd89c20eb7d10ccd9d4795
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.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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.maximus.missinginformation.nysoh.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

🔍 APKID ANALYSIS

FILE	DETAILS		
classes.dex	**FINDINGS**		**DETAILS**
	Anti-VM Code		Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check SIM operator check network operator name check
	Compiler		r8 without marker (suspicious)

FILE	DETAILS
classes2.dex	**FINDINGS** / **DETAILS** Anti-VM Code: Build.FINGERPRINT check, Build.MODEL check, Build.MANUFACTURER check, Build.PRODUCT check, Build.HARDWARE check, Build.TAGS check, possible VM check Anti Debug Code: Debug.isDebuggerConnected() check Compiler: r8 without marker (suspicious)
classes3.dex	**FINDINGS** / **DETAILS** 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

🔍 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	Service (com.maximus.missinginformation.api.NYSOHFirebaseMessagingService) 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.
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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/Analytics.java com/adobe/marketing/mobile/AnalyticsCore.java com/adobe/marketing/mobile/AnalyticsExtension.java com/adobe/marketing/mobile/AnalyticsHitSchema.java com/adobe/marketing/mobile/AnalyticsHitsDatabase.java com/adobe/marketing/mobile/AnalyticsListenerAnalyticsRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerGenericTrackRequestContent.java com/adobe/marketing/mobile/AnalyticsListenerHubSharedState.java com/adobe/marketing/mobile/AnalyticsListenerRulesEngineResponseContent.java com/adobe/marketing/mobile/AnalyticsState.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidDataStore.java com/adobe/marketing/mobile/AndroidDatabase.java com/adobe/marketing/mobile/AndroidDatabaseService.java com/adobe/marketing/mobile/AndroidDeepLinkService.java com/adobe/marketing/mobile/AndroidEncodingService.java com/adobe/marketing/mobile/AndroidEventHistory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/AndroidEventHistoryDatabase.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/AndroidJsonUtility.java com/adobe/marketing/mobile/AndroidLoggingService.java com/adobe/marketing/mobile/AndroidNetworkService.java com/adobe/marketing/mobile/AndroidNetworkServiceOverrider.java com/adobe/marketing/mobile/AndroidSystemInfoService.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/ConfigurationData.java com/adobe/marketing/mobile/ConfigurationDownloader.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/ConfigurationSharedStateIdentity.java com/adobe/marketing/mobile/ContextDataUtil.java com/adobe/marketing/mobile/Core.java com/adobe/marketing/mobile/DispatcherAnalyticsRequestContentIdentity.java com/adobe/marketing/mobile/Event.java com/adobe/marketing/mobile/EventBus.java com/adobe/marketing/mobile/EventData.java com/adobe/marketing/mobile/EventDataFlattener.java com/adobe/marketing/mobile/EventHub.java com/adobe/marketing/mobile/Extension.java com/adobe/marketing/mobile/ExtensionA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pi.java com/adobe/marketing/mobile/ExtensionListener.java
				com/adobe/marketing/mobile/FileUtil.java
				com/adobe/marketing/mobile/FloatingButtonView.java
				com/adobe/marketing/mobile/FullscreenMessageActivity.java
				com/adobe/marketing/mobile/HexStringUtil.java
				com/adobe/marketing/mobile/HitQueue.java
				com/adobe/marketing/mobile/Identity.java
				com/adobe/marketing/mobile/IdentityCore.java
				com/adobe/marketing/mobile/IdentityExtension.java
				com/adobe/marketing/mobile/IdentityHitSchema.java
				com/adobe/marketing/mobile/IdentityHitsDatabase.java
				com/adobe/marketing/mobile/LifecycleCore.java
				com/adobe/marketing/mobile/LifecycleExtension.java
				com/adobe/marketing/mobile/LifecycleMetricsBuilder.java
				com/adobe/marketing/mobile/LifecycleSession.java
				com/adobe/marketing/mobile/LifecycleV2DataStoreCache.java
				com/adobe/marketing/mobile/LifecycleV2MetricsBuilder.java
				com/adobe/marketing/mobile/ListenerRulesEngineResponseContentSignal.java
				com/adobe/marketing/mobile/ListenerRulesResponseContentProfile.java
				com/adobe/marketing/mobile/ListenerUserProfileRequestProfile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/ListenerUsEPPfileRequestReset.java
				com/adobe/marketing/mobile/LocalNotificationHandler.java
				com/adobe/marketing/mobile/Matcher.java
				com/adobe/marketing/mobile/MobileCore.java
				com/adobe/marketing/mobile/Module.java
				com/adobe/marketing/mobile/PermissiveVariantSerializer.java
				com/adobe/marketing/mobile/PersistentProfileData.java
				com/adobe/marketing/mobile/RangedResolver.java
				com/adobe/marketing/mobile/RemoteDownloader.java
				com/adobe/marketing/mobile/RuleConditionHistorical.java
				com/adobe/marketing/mobile/RuleConsequence.java
				com/adobe/marketing/mobile/RulesEngine.java
				com/adobe/marketing/mobile/SignalCore.java
				com/adobe/marketing/mobile/SignalExtension.java
				com/adobe/marketing/mobile/SignalHitSchema.java
				com/adobe/marketing/mobile/SignalHitsDatabase.java
				com/adobe/marketing/mobile/SignalTemplate.java
				com/adobe/marketing/mobile/StringEncoder.java
				com/adobe/marketing/mobile/StringUtils.java
				com/adobe/marketing/mobile/TLSSocketFactory.java
				com/adobe/marketing/mobile/TimerState

NO	ISSUE	SEVERITY	STANDARDS	FILES
				.java com/adobe/marketing/mobile/URLBuilder.java com/adobe/marketing/mobile/UrlUtilities.java com/adobe/marketing/mobile/UserProfile.java com/adobe/marketing/mobile/UserProfileCore.java com/adobe/marketing/mobile/UserProfileExtension.java com/adobe/marketing/mobile/V4ToV5Migration.java com/adobe/marketing/mobile/VisitorID.java com/adobe/marketing/mobile/ZipBundleHandler.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideEx

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ception.java com/bumptech/glide/load/engine/Source Generator.java
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/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitm

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/maximus/missinginformation/api/NYSOHFirebaseMessagingService.java com/maximus/missinginformation/ui/fragments/SubmissionSelectionFragment.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/maximus/missinginformation/ui/fragments/SubmitDocumentsFragment.java com/maximus/missinginformation/ui/fragments/TermsOfUseFragment.java com/maximus/missinginformation/util/AppLifecycleObserver.java com/maximus/missinginformation/util/MaximusPrefs.java com/maximus/missinginformation/util/PhotoEncryptor.java com/mellissa/addressautocomplete/MelissaAutocompleteTextView.java com/stfalcon/imageviewer/StfalconImageViewer.java com/theartofdev/edmodo/cropper/BitmapUtils.java com/theartofdev/edmodo/cropper/CropImageActivity.java com/theartofdev/edmodo/cropper/CropOverlayView.java com/webtrends/mobile/analytics/WTConfig.java com/webtrends/mobile/analytics/WTCoreClientInfo.java com/webtrends/mobile/analytics/WTCoreConfigSetting.java com/webtrends/mobile/analytics/WTCoreEventBatch.java com/webtrends/mobile/analytics/WTCoreEventSendTask.java com/webtrends/mobile/analytics/WTCoreEventStore.java com/webtrends/mobile/analytics/WTCoreHttpClient.java com/webtrends/mobile/analytics/WTCoreKeyValuePairs.java com/webtrends/mobile/analytics/WTCoreLog.java com/webtrends/mobile/analytics/WTCoreMapToJsonHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/webtrends/mobile/analytics/WTCore RcsConfig.java
				com/webtrends/mobile/analytics/WTCore RcsPollTask.java
				com/webtrends/mobile/analytics/WTCore SendHealthStatus.java
				com/webtrends/mobile/analytics/WTCore TaskInitialize.java
				com/webtrends/mobile/analytics/WTCore TaskLoadConfig.java
				com/webtrends/mobile/analytics/WTCore TaskMigration.java
				com/webtrends/mobile/analytics/WTCore TaskProcessEvent.java
				com/webtrends/mobile/analytics/WTData Collector.java
				com/webtrends/mobile/analytics/WTOpt Button.java
				com/webtrends/mobile/analytics/WTOpt Database.java
				com/webtrends/mobile/analytics/WTOptE ditText.java
				com/webtrends/mobile/analytics/WTOptF actor.java
				com/webtrends/mobile/analytics/WTOptI mageCache.java
				com/webtrends/mobile/analytics/WTOptI mageFactor.java
				com/webtrends/mobile/analytics/WTOpt MultivariateFactor.java
				com/webtrends/mobile/analytics/WTOpt Project.java
				com/webtrends/mobile/analytics/WTOptS tore.java
				com/webtrends/mobile/analytics/WTOptT askDownloadImage.java
				com/webtrends/mobile/analytics/WTOptT askPollServer.java
				com/webtrends/mobile/analytics/WTOptT est.java
				com/webtrends/mobile/analytics/WTOptT

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/webtrends/mobile/analytics/WTOptextView.java com/webtrends/mobile/analytics/WTOptWebView.java com/webtrends/mobile/analytics/WTOptimizeManager.java com/webtrends/mobile/analytics/WTPersistentCookieStore.java com/webtrends/mobile/analytics/WTReferrerReceiver.java com/webtrends/mobile/analytics/WTTask.java com/webtrends/mobile/analytics/WTTaskReferrerCheck.java com/webtrends/mobile/analytics/WTWebViewClient.java io/github/inflationx/calligraphy3/ReflectionUtils.java io/github/inflationx/calligraphy3/TypefaceUtils.java io/github/inflationx/viewpump/internal/ReflectionUtils.java io/realm/BaseRealm.java io/realm/DynamicRealm.java io/realm/Realm.java io/realm/RealmCache.java io/realm/RealmObject.java io/realm/RealmResults.java io/realm/internal/FinalizerRunnable.java io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/Util.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java org/opencv/android/AsyncServiceHelper.java org/opencv/android/Camera2Renderer.java org/opencv/android/CameraBridgeViewBase.java org/opencv/android/CameraGLRendererB

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/opencv/android/CameraGLRendererBase.java org/opencv/android/CameraGLSurfaceView.java org/opencv/android/CameraRenderer.java org/opencv/android/FpsMeter.java org/opencv/android/StaticHelper.java rx/internal/util/IndexedRingBuffer.java rx/internal/util/RxJavaPluginUtils.java rx/internal/util/RxRingBuffer.java timber/log/Timber.java
				com/adobe/marketing/mobile/AnalyticsConstants.java com/adobe/marketing/mobile/AndroidUIService.java com/adobe/marketing/mobile/App.java com/adobe/marketing/mobile/ConfigurationConstants.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/CoreConstants.java com/adobe/marketing/mobile/DataMarshaller.java com/adobe/marketing/mobile/EventDataKeys.java com/adobe/marketing/mobile/IdentityConstants.java com/adobe/marketing/mobile/LifecycleConstants.java com/adobe/marketing/mobile/Matcher.java com/adobe/marketing/mobile/RuleConditionGroup.java com/adobe/marketing/mobile/UserProfileConstants.java com/adobe/marketing/mobile/V4ToV5Migration.java com/adobe/marketing/mobile/services/ui

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	/AndroidUIService.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/maximus/missinginformation/BuildConfig.java com/maximus/missinginformation/api/DisplayTextResponse.java com/maximus/missinginformation/api/FaqsResponse.java com/maximus/missinginformation/ui/activities/BaseActivity.java com/maximus/missinginformation/ui/fragments/DatePickerDialogFragment.java com/maximus/missinginformation/util/DatabaseManager.java com/maximus/missinginformation/util/MaximusPrefs.java com/mellissa/addressautocomplete/Constants.java com/mellissa/addressautocomplete/util/KeyUtility.java com/webtrends/mobile/analytics/WTCoreConstants.java com/webtrends/mobile/analytics/WTCoreSession.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java rx/internal/schedulers/NewThreadWorker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/maximus/missinginformation/documentScanner/model/DocumentManager.java com/maximus/missinginformation/documentScanner/model/Image.java com/maximus/missinginformation/documentScanner/util/ImageFilePath.java com/maximus/missinginformation/util/CompressImage.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/maximus/missinginformation/api/ApiClient.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/theartofdev/edmodo/cropper/BitmapUtils.java com/theartofdev/edmodo/cropper/CropImageActivity.java
6	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/AndroidDatabase.java com/adobe/marketing/mobile/AndroidEventHistoryDatabase.java com/adobe/marketing/mobile/services/SQLiteDatabaseHelper.java com/webtrends/mobile/analytics/WTCoreEventDb.java com/webtrends/mobile/analytics/WTOptDatabase.java
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/maximus/missinginformation/util/PhotoEncryptor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Calling Cipher.getInstance("AES") will return AES ECB mode by default. 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	com/mellissa/addressautocomplete/util/KeyUtility.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/webtrends/mobile/analytics/BuildConfig.java
10	This App use Realm Database with encryption.	secure	OWASP MASVS: MSTG-CRYPTO-1	com/maximus/missinginformation/util/DatabaseManager.java
11	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/StringEncoder.java
12	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	com/webtrends/mobile/analytics/WTOptImageCache.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/ConfigurationExtension.java com/adobe/marketing/mobile/FileUtil.java com/adobe/marketing/mobile/services/ui/MessageWebViewClient.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/getkeepsafe/relinker/elf/ElfParser.java com/maximus/missinginformation/ui/fragments/AssistorIDProofingReviewFragment.java com/maximus/missinginformation/ui/fragments/SubmitDocumentsFragment.java com/maximus/missinginformation/util/PhotoEncryptor.java com/mellissa/addressautocomplete/history/DefaultAutocompleteHistoryManager.java okio/Okio.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java org/threeten/bp/chrono/HijrahDate.java
00091	Retrieve data from broadcast	collection	com/adobe/marketing/mobile/LocalNotificationHandler.java com/webtrends/mobile/analytics/WTReferrerReceiver.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/navgde/grammaticalinflectionapi/data/ContentResolverKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/RemoteDownloader.java com/getkeepsafe/relinker/ReLinkerInstance.java com/maximus/missinginformation/documentScanner/activity/DocumentPreviewActivity.java com/maximus/missinginformation/documentScanner/activity/DocumentScannerActivity.java com/maximus/missinginformation/documentScanner/model/Image.java com/maximus/missinginformation/ui/fragments/AssistorIDProofingReviewFragment.java com/maximus/missinginformation/ui/fragments/AssistorSubmitDocumentsFragment.java com/maximus/missinginformation/ui/fragments/SubmissionSelectionFragment.java com/maximus/missinginformation/ui/fragments/SubmitDocumentsFragment.java com/maximus/missinginformation/util/CompressImage.java com/maximus/missinginformation/util/PhotoEncryptor.java com/webtrends/mobile/analytics/WTOptImageCache.java io/realm/RealmConfiguration.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java org/opencv/android/Utils.java
00096	Connect to a URL and set request method	command network	com/webtrends/mobile/analytics/WTCoreHttpClient.java
00094	Connect to a URL and read data from it	command network	com/webtrends/mobile/analytics/WTCoreHttpClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mellissa/addressautocomplete/network/MellissaHttpUrlConnectionMapsHttpClient.java com/webtrends/mobile/analytics/WTOptTaskDownloadImage.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/webtrends/mobile/analytics/WTOptTaskDownloadImage.java
00183	Get current camera parameters and change the setting.	camera	com/maximus/missinginformation/documentScanner/view/ScanSurfaceView.java org/opencv/android/CameraRenderer.java org/opencv/android/JavaCameraView.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adobe/marketing/mobile/AndroidDeepLinkService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/AEPMessage.java com/adobe/marketing/mobile/services/ui/AndroidUIService.java com/maximus/missinginformation/customgallery/CustomGalleryActivity.java com/maximus/missinginformation/ui/fragments/ContactFragment.java com/maximus/missinginformation/ui/fragments/ContactPreferencesFragment.java com/maximus/missinginformation/ui/fragments/ProfilesListFragment.java com/maximus/missinginformation/ui/fragments/RenewAlertBottomSheetDialogFragment.java com/maximus/missinginformation/ui/fragments/SubmitBottomSheetDialogFragment.java com/maximus/missinginformation/ui/fragments/SubmitDocumentsFragment.java com/maximus/missinginformation/ui/fragments/TermsOfUseFragment.java com/maximus/missinginformation/util/LinkManager.java com/webtrends/mobile/analytics/WTDataCollector.java org/opencv/android/AsyncServiceHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/adobe/marketing/mobile/AndroidDeepLinkService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/AEPMessage.java com/adobe/marketing/mobile/services/ui/AndroidUIService.java com/maximus/missinginformation/customgallery/CustomGalleryActivity.java com/maximus/missinginformation/ui/fragments/ContactFragment.java com/maximus/missinginformation/ui/fragments/ContactPreferencesFragment.java com/maximus/missinginformation/ui/fragments/ProfilesListFragment.java com/maximus/missinginformation/ui/fragments/RenewAlertBottomSheetDialogFragment.java com/maximus/missinginformation/ui/fragments/SubmitBottomSheetDialogFragment.java com/maximus/missinginformation/ui/fragments/TermsOfUseFragment.java com/maximus/missinginformation/util/LinkManager.java com/webtrends/mobile/analytics/WTDataCollector.java
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/AndroidSystemInfoService.java com/adobe/marketing/mobile/services/DeviceInfoService.java com/webtrends/mobile/analytics/WTCoreClientInfo.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00202	Make a phone call	control	com/maximus/missinginformation/ui/fragments/ContactFragment.java com/maximus/missinginformation/ui/fragments/ContactPreferencesFragment.java com/maximus/missinginformation/ui/fragments/ProfilesListFragment.java com/maximus/missinginformation/ui/fragments/SubmitBottomSheetDialogFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	com/maximus/missinginformation/ui/fragments/ContactFragment.java com/maximus/missinginformation/ui/fragments/ContactPreferencesFragment.java com/maximus/missinginformation/ui/fragments/ProfilesListFragment.java com/maximus/missinginformation/ui/fragments/SubmitBottomSheetDialogFragment.java
00002	Open the camera and take picture	camera	com/maximus/missinginformation/documentScanner/view/ScanSurfaceView.java
00125	Check if the given file path exist	file	com/maximus/missinginformation/ui/fragments/SubmitDocumentsFragment.java
00132	Query The ISO country code	telephony collection	com/webtrends/mobile/analytics/WTCoreClientInfo.java
00192	Get messages in the SMS inbox	sms	com/maximus/missinginformation/documentScanner/util/ImageFilePath.java
00163	Create new Socket and connecting to it	socket	com/adobe/marketing/mobile/services/HttpConnectionHandler.java
00009	Put data in cursor to JSON object	file	com/webtrends/mobile/analytics/WTOptDatabase.java
00012	Read data and put it into a buffer stream	file	com/maximus/missinginformation/ui/fragments/AssistorIDProofingReviewFragment.java
00187	Query a URI and check the result	collection sms calllog calendar	com/navgde/grammaticalinflectionapi/data/ContentResolverKt.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/539694057856/namespaces/firebase:fetch?key=AIzaSyBxoCx-Y-qvwTI6pXZy7StDAOLRTmKm72E. This is indicated by the response: {'state': 'NO_TEMPLATE'}

⁞⁞ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
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
ots.optimize.webtrends.com	ok	**IP:** 135.237.225.159 **Country:** United States of America **Region:** Illinois **City:** Naperville **Latitude:** 41.791512 **Longitude:** -88.163277 **View:** Google Map
scs.webtrends.com	ok	No Geolocation information available.
api.nysoh-maximus-mobileapi.com	ok	**IP:** 18.238.96.81 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
realm.io	ok	**IP:** 13.224.53.90 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ots.optimize.com	ok	**IP:** 3.228.19.23 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.3.85.32 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
rcs.webtrends.com	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
testingemail@testing.com	com/maximus/missinginformation/ui/fragments/ContactPreferencesFragment.java
test@test.com	com/maximus/missinginformation/ui/fragments/LoginStep1Fragment.java

🕵 TRACKERS

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
Webtrends	Analytics	https://reports.exodus-privacy.eu.org/trackers/129

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBxoCx-Y-qvwTI6pXZy7StDAOLRTmKm72E"

POSSIBLE SECRETS

"google_crash_reporting_api_key" : "AIzaSyBxoCx-Y-qvwTI6pXZy7StDAOLRTmKm72E"

"webtrends_key" : "dcs2225v0rcesow8m3e4nhyz5_7e2e"

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

470fa2b4ae81cd56ecbcda9735803434cec591fa

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

Ek9vZFfmIH9M0vXuaQAxB8eXieEasYUo6erlzQi6

394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F80818283848586878889898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: NYSOH Mobile Upload

Score: 4.805697 **Installs:** 100,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** com.maximus.missinginformation.nysoh

Developer Details: MAXIMUS, MAXIMUS, None, https://nystateofhealth.ny.gov, mobile@maximus.com,

Release Date: Oct 27, 2019 **Privacy Policy:** Privacy link

Description:

When you apply for health insurance through the NY State of Health (NYSOH) marketplace, you may need to provide supporting documents to complete your application. With the NYSOH Mobile App, you can take a picture of your documents, or choose a photo of your documents from your device's album, and upload it to your account. The NYSOH Mobile App now also allows you to view your eligibility and enrollment dates, program information, and more. The NYSOH Mobile App is quick and easy to use. Following a simple log in from your phone or tablet, you can choose to upload a document to your account or navigate to your account overview to view your account information. Do you have questions or feedback? Call us. We can help! Toll-free number: 1.855.355.5777 TTY: 1.800.662.1220 NYSOH Mobile Upload is for New York residents only.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-31 02:35:33	Generating Hashes	OK
2025-08-31 02:35:33	Extracting APK	OK
2025-08-31 02:35:33	Unzipping	OK
2025-08-31 02:35:33	Parsing APK with androguard	OK
2025-08-31 02:35:33	Extracting APK features using aapt/aapt2	OK
2025-08-31 02:35:33	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 02:35:35	Parsing AndroidManifest.xml	OK
2025-08-31 02:35:35	Extracting Manifest Data	OK
2025-08-31 02:35:35	Manifest Analysis Started	OK

2025-08-31 02:35:35	Performing Static Analysis on: NYSOH Upload (com.maximus.missinginformation.nysoh)	OK
2025-08-31 02:35:36	Fetching Details from Play Store: com.maximus.missinginformation.nysoh	OK
2025-08-31 02:35:37	Checking for Malware Permissions	OK
2025-08-31 02:35:37	Fetching icon path	OK
2025-08-31 02:35:37	Library Binary Analysis Started	OK
2025-08-31 02:35:37	Reading Code Signing Certificate	OK
2025-08-31 02:35:37	Running APKiD 2.1.5	OK
2025-08-31 02:35:42	Detecting Trackers	OK
2025-08-31 02:35:45	Decompiling APK to Java with JADX	OK
2025-08-31 02:39:07	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-31 02:39:07	Decompiling classes2.dex with JADX	OK

2025-08-31 02:40:51	Decompiling classes.dex with JADX	OK
2025-08-31 02:41:01	Decompiling classes3.dex with JADX	OK
2025-08-31 02:41:10	Decompiling classes2.dex with JADX	OK
2025-08-31 02:41:23	Decompiling classes.dex with JADX	OK
2025-08-31 02:41:35	Decompiling classes3.dex with JADX	OK
2025-08-31 02:41:46	Converting DEX to Smali	OK
2025-08-31 02:41:46	Code Analysis Started on - java_source	OK
2025-08-31 02:41:49	Android SBOM Analysis Completed	OK
2025-08-31 02:43:30	Android SAST Completed	OK
2025-08-31 02:43:30	Android API Analysis Started	OK
2025-08-31 02:43:44	Android API Analysis Completed	OK

2025-08-31 02:43:44	Android Permission Mapping Started	OK
2025-08-31 02:43:56	Android Permission Mapping Completed	OK
2025-08-31 02:43:56	Android Behaviour Analysis Started	OK
2025-08-31 02:44:14	Android Behaviour Analysis Completed	OK
2025-08-31 02:44:14	Extracting Emails and URLs from Source Code	OK
2025-08-31 02:44:19	Email and URL Extraction Completed	OK
2025-08-31 02:44:19	Extracting String data from APK	OK
2025-08-31 02:44:19	Extracting String data from Code	OK
2025-08-31 02:44:19	Extracting String values and entropies from Code	OK
2025-08-31 02:44:24	Performing Malware check on extracted domains	OK
2025-08-31 02:44:29	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.