MOBSF

ANDROID STATIC ANALYSIS REPORT

Update service (8.1.1.2)

File Name:	mSpy.apk
Package Name:	update.service.android
Scan Date:	Aug. 17, 2024, 4:39 p.m.

App Security Score: 53/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	26	2	2	2

FILE INFORMATION

File Name: mSpy.apk
Size: 17.52MB

MD5: 34760b1b52e8cb9bc6e603c211453c78
SHA1: 0a20fb2e1b5883a2b79b356b8732f0c0f03158ff
SHA256: 57de2876ab41fc0afdcfd43f393585ac08941d3be8bac697958b5cd28e58acf5

APP INFORMATION

App Name: Update service
Package Name: update.service.android
Main Activity: update.service.core.ui.main.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 8.1.1.2
Android Version Code: 637

APP COMPONENTS

Activities: 8
Services: 18
Receivers: 17
Providers: 3
Exported Activities: 3
Exported Services: 2
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=MS, ST=ms, L=ms, O=ms, OU=ms, CN=ms
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-08-01 12:37:54+00:00
Valid To: 2048-07-25 12:37:54+00:00
Issuer: C=MS, ST=ms, L=ms, O=ms, OU=ms, CN=ms
Serial Number: 0x53f4801d
Hash Algorithm: sha256
md5: 022b6683dbb63fb1fffc5d6a9fd6d7ca
sha1: 1ecc7f67bbd1bfab97addcb05a496bca7b6b135f
sha256: 1809332e0cd73548c83960217a0041917c9c2fae20da11b0c9dce0897c20771f
sha512: 3ca451e6f2655ecc4c1c184e29dff63e37557eae707393a914a8f88de2388dbfa8bfa7679db4d3b6032e3ab7b8cd2b846f6f59b5583fdc6f133443d3b8d20377
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 132c83b57d165df32853f05b25e3808b3fed44e414671e12fb6eefe2a638e63c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.NEW_OUTGOING_CALL	unknown	Unknown permission	Unknown permission from android reference
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_USER_DICTIONARY	dangerous	read user-defined dictionary	Allows an application to read any private words, names and phrases that the user may have stored in the user dictionary.
android.permission.WRITE_USER_DICTIONARY	normal	write to user-defined dictionary	Allows an application to write new words into the user dictionary.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.factory.permission.KEYSTRING	unknown	Unknown permission	Unknown permission from android reference
com.sec.testingsettings.permission.KEYSTRING	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.app.servicemodeapp.permission.KEYSTRING	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_CONFIGURATION	SignatureOrSystem	change your UI settings	Allows an application to change the current configuration, such as the locale or overall font size.
android.permission.INTERNAL_SYSTEM_WINDOW	signature	display unauthorised windows	Allows the creation of windows that are intended to be used by the internal system user interface. Not for use by common applications.
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.CALL_PRIVILEGED	SignatureOrSystem	directly call any phone numbers	Allows the application to call any phone number, including emergency numbers, without your intervention. Malicious applications may place unnecessary and illegal calls to emergency services.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
update.service.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.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.TAGS check
SIM operator check
network operator name check
device ID check
ro.kernel.qemu check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() 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
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check network operator name check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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: 1 | WARNING: 15 | 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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Activity-Alias (update.service.core.ui.CompleteActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (update.service.core.ui.block.BlockActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (update.service.core.ui.update.UpdateBuildActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Service (update.service.core.services.CallFilteringService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_SCREENING_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.
7	Broadcast Receiver (update.service.core.receiver.UpdateServiceReceiver) is not Protected. [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.
8	Broadcast Receiver (update.service.core.receiver.PhoneAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
9	Broadcast Receiver (update.service.core.receiver.CallReceiver) is not Protected. [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.
10	Broadcast Receiver (update.service.core.receiver.SmsReceiver) is not Protected. [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.
11	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.
12	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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	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.
14	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.
15	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
16	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/amplitude/api/AmplitudeClient.java com/qonversion/android/sdk/automations/internal/macros/ScreenProcessor.java com/qonversion/android/sdk/automations/mvp/ScreenFragment.java com/qonversion/android/sdk/dto/properties/QUserProperty.java com/qonversion/android/sdk/internal/Constants.java com/qonversion/android/sdk/internal/api/ApiHeadersProvider.java com/qonversion/android/sdk/internal/dto/SendPropertiesResult.java com/qonversion/android/sdk/internal/dto/config/PrimaryConfig.java com/qonversion/android/sdk/internal/dto/request/CrashRequest.java com/qonversion/android/sdk/internal/dto/request/data/UserPropertyRequestData.java com/qonversion/android/sdk/internal/extractor/SkuDetailsTokenExtractor.java com/qonversion/android/sdk/internal/storage/LaunchResultCacheWrapperKt.java com/qonversion/android/sdk/internal/storage/PurchasesCache.java com/qonversion/android/sdk/internal/storage/TokenStorage.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java update/service/android/BuildConfig.java update/service/core/initializers/AmplitudeInitializer.java update/service/core/ui/stepper/install/setting/notificationListener/NotificationListenerSettingFragment.java update/service/data/local/db/model/KeyLoggerEntity.java update/service/data/local/db/model/WifiNetworkEntity.java update/service/data/local/db/model/facebook/FacebookUserEntity.java update/service/data/remote/api/model/request/UploadStartRequest.java update/service/data/remote/api/model/request/sensor/KeyLoggerRequest.java update/service/data/remote/api/model/request/sensor/WifiNetworkRequest.java update/service/data/remote/api/model/request/sensor/facebook/FacebookUserRequest.java update/service/data/remote/api/model/request/sensor/skype/SkypeCallRequest.java update/service/data/remote/api/model/request/sensor/whatsapp/WhatsAppCallRequest.java update/service/data/remote/api/model/request/sensor/whatsapp/WhatsAppMessageRequest.java update/service/data/remote/api/model/response/instagram/InstagramInviterResponseEntity.java update/service/data/remote/api/model/response/instagram/InstagramUserResponseEntity.java update/service/data/sensor/accessibility/grabber/InstagramGrabberAccessibilitySensorImpl.java update/service/data/worker/root/SamsungEmailRootWorker.java update/service/domain/model/local/KeyLogger.java update/service/domain/model/local/WifiNetwork.java update/service/domain/model/local/facebook/FacebookUser.java update/service/domain/model/remote/instagram/InstagramMessageResponse.java update/service/domain/model/remote/instagram/UserResponse.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	by/kirich1409/viewbindingdelegate/LifecycleViewBindingProperty.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/api/AmplitudeLog.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1bSDK.java com/appsflyer/internal/AFd1aSDK.java com/appsflyer/internal/AFd1bSDK.java com/appsflyer/internal/AFd1cSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1lSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFd1xSDK.java com/appsflyer/internal/AFe1tSDK.java com/appsflyer/internal/AFf1dSDK.java com/github/anrwatchdog/ANRWatchDog.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/journeyapps/barcodescanner/camera/CameraConfigurationUtils.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/journeyapps/barcodescanner/camera/CameraManager.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/neovisionaries/ws/client/SNIHelper.java com/qonversion/android/sdk/Qonversion.java com/qonversion/android/sdk/QonversionConfig.java com/qonversion/android/sdk/internal/logger/ExceptionHandler.java com/qonversion/android/sdk/internal/logger/QExceptionManager$sendCrashReportsInBackground$1$1$1$2.java com/qonversion/android/sdk/internal/logger/QExceptionManager.java com/stericson/RootShell/containers/RootClass.java com/stericson/RootTools/RootTools.java dagger/android/AndroidInjection.java timber/log/Timber.java
3	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/appsflyer/internal/AFa1zSDK.java com/qonversion/android/sdk/internal/IncrementalDelayCalculator.java com/qonversion/android/sdk/internal/di/module/ManagersModule.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/amplitude/api/PinnedAmplitudeClient.java com/qonversion/android/sdk/internal/di/module/NetworkModule.java update/service/data/di/DataModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/stericson/RootShell/RootShellUtil.java update/service/preference_data/repository/PreferenceRepositoryImpl.java update/service/preference_domain/repository/PreferenceRepository.java update/service/preference_domain/usecase/PhoneInfoUseCase.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/amplitude/api/DatabaseHelper.java update/service/data/worker/root/FacebookRootWorker.java update/service/data/worker/root/GmailRootWorker.java update/service/data/worker/root/InstagramRootWorker.java update/service/data/worker/root/KikRootWorker.java update/service/data/worker/root/LineRootWorker.java update/service/data/worker/root/SamsungBrowserRootWorker.java update/service/data/worker/root/SamsungEmailRootWorker.java update/service/data/worker/root/SnapchatRootWorker.java update/service/data/worker/root/TelegramRootWorker.java update/service/data/worker/root/ViberRootWorker.java update/service/data/worker/root/WhatsappRootWorker.java
7	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/stericson/RootTools/internal/RootToolsInternalMethods.java update/service/data/manager/PhoneInfoManager.java update/service/preference_data/repository/StorageRepositoryImpl.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	update/service/android/BuildConfig.java
9	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/journeyapps/barcodescanner/CaptureManager.java update/service/data/manager/UsageAppStatsManager.java
10	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/stericson/RootTools/internal/Installer.java tgnet/Utilities.java update/service/data/util/CryptUtilImpl.java update/service/data/util/SecurityUtilImpl.java update/service/data/worker/root/SkypeRootWorker.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/neovisionaries/ws/client/HandshakeReader.java tgnet/Utilities.java
12	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/stericson/RootTools/internal/RootToolsInternalMethods.java
13	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/amplitude/eventexplorer/EventExplorerInfoActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	19/24	android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CALL_LOG, android.permission.READ_PHONE_STATE, android.permission.GET_ACCOUNTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_SETTINGS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA
Other Common Permissions	17/45	android.permission.PROCESS_OUTGOING_CALLS, android.permission.CALL_PHONE, android.permission.WRITE_SMS, android.permission.WRITE_CONTACTS, android.permission.READ_CALENDAR, android.permission.CHANGE_WIFI_STATE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.CHANGE_NETWORK_STATE, android.permission.PACKAGE_USAGE_STATS, com.google.android.gms.permission.AD_ID, 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
journeyapps.com	ok	**IP:** 3.165.206.74 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
scdn-ssettings.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
api.qonversion.io	ok	**IP:** 104.22.7.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
api.eu.amplitude.com	ok	**IP:** 18.198.65.112 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
sdk-logs.qonversion.io	ok	**IP:** 104.22.6.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 3.165.206.95 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 3.165.206.9 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
mobile-gw.thd.cc	ok	**IP:** 104.26.5.141 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
sdlsdk.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
i.instagram.com	ok	**IP:** 31.13.84.52 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
api2.amplitude.com	ok	**IP:** 44.228.30.247 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
documentation.qonversion.io	ok	**IP:** 104.22.7.135 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyDKlzr_PerwLnJsoiaoik9EkvZF185s1ps"
"google_crash_reporting_api_key" : "AIzaSyDKlzr_PerwLnJsoiaoik9EkvZF185s1ps"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
7d73d21f1bd82c9e5268b6dcf9fde2cb
3071c8717539de5d5353f4c8cd59a032
c7c0e3677d615ffd6b795c948d3bb4d9
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
470fa2b4ae81cd56ecbcda9735803434cec591fa
7ee895272396129c556441f4bd20b346
dcd70338f3efccf02c9d10971278eec3
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
C71CAEB9C6B1C9048E6C522F70F13F73980D40238E3E21C14934D037563D930F48198A0AA7C14058229493D22530F4DBFA336F6E0AC925139543AED44CCE7C3720FD51F69458705AC68CD4FE6B6B13ABDC9746512969328454F18FAF8C595F642477FE96BB2A941D5BCD1D4AC8CC49880708FA9B378E3C4F3A9060BEE67CF9A4A4A695811051907E162753B56B0F6B410DBA74D8A84B2A14B3144E0EF1284754FD17ED950D5965B4B9DD46582DB1178D169C6BC465B0D6FF9CA3928FEF5B9AE4E418FC15E83EBEA0F87FA9FF5EED70050DED2849F47BF959D956850CE929851F0D8115F635B105EE2E4E15D04B2454BF6F4FADF034B10403119CD8E3B92FCC5B
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

SCAN LOGS

Timestamp	Event	Error
2024-08-17 16:39:52	Generating Hashes	OK
2024-08-17 16:39:52	Extracting APK	OK
2024-08-17 16:39:52	Unzipping	OK
2024-08-17 16:39:53	Getting Hardcoded Certificates/Keystores	OK
2024-08-17 16:39:55	Parsing AndroidManifest.xml	OK
2024-08-17 16:39:55	Parsing APK with androguard	OK
2024-08-17 16:39:56	Extracting Manifest Data	OK
2024-08-17 16:39:56	Performing Static Analysis on: Update service (update.service.android)	OK
2024-08-17 16:39:56	Fetching Details from Play Store: update.service.android	OK
2024-08-17 16:39:56	Manifest Analysis Started	OK
2024-08-17 16:39:56	Checking for Malware Permissions	OK
2024-08-17 16:39:56	Fetching icon path	OK
2024-08-17 16:39:56	Library Binary Analysis Started	OK
2024-08-17 16:39:56	Reading Code Signing Certificate	OK

2024-08-17 16:39:56	Running APKiD 2.1.5	OK
2024-08-17 16:40:01	Updating Trackers Database....	OK
2024-08-17 16:40:01	Detecting Trackers	OK
2024-08-17 16:40:05	Decompiling APK to Java with jadx	OK
2024-08-17 16:40:50	Converting DEX to Smali	OK
2024-08-17 16:40:50	Code Analysis Started on - java_source	OK
2024-08-17 16:49:35	Android SAST Completed	OK
2024-08-17 16:49:35	Android API Analysis Started	OK
2024-08-17 16:57:38	Android Permission Mapping Started	OK
2024-08-17 17:08:16	Android Permission Mapping Completed	OK
2024-08-17 17:08:19	Finished Code Analysis, Email and URL Extraction	OK
2024-08-17 17:08:19	Extracting String data from APK	OK
2024-08-17 17:08:19	Extracting String data from Code	OK
2024-08-17 17:08:19	Extracting String values and entropies from Code	OK
2024-08-17 17:08:24	Performing Malware check on extracted domains	OK

2024-08-17 17:08:27	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.