ANDROID STATIC ANALYSIS REPORT

Contact Tracing (1.3.8)

File Name:	Contact Tracing 1.3.8.apk
Package Name:	com.piusworks.contact
Average CVSS Score:	6.2
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	8/285

FILE INFORMATION

File Name: Contact Tracing 1.3.8.apk
Size: 8.63MB
MD5: b5254ec24a8d48cb5f3be60c00145587
SHA1: 119b36e083c6226ce49d01003434ce27163ae60b
SHA256: 86e4c5370f1c5286b7f0aa76c5cc216ec3e8d43c11125fa1eff69632b596efc7

APP INFORMATION

App Name: Contact Tracing
Package Name: com.piusworks.contact
Main Activity: com.piusworks.contact.MainActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 1.3.8
Android Version Code: 13

APP COMPONENTS

Activities: 10
Services: 12
Receivers: 8
Providers: 5
Exported Activities: 0
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=00, ST=CA, L=San Francisco, O=Mobile Development, OU=Programming, CN=Alvin Desuasido
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-27 16:00:46+00:00
Valid To: 2045-03-21 16:00:46+00:00
Issuer: C=00, ST=CA, L=San Francisco, O=Mobile Development, OU=Programming, CN=Alvin Desuasido
Serial Number: 0x203467b5
Hash Algorithm: sha256
md5: 1713a530b6a3b01e0ffa6437cb03e960
sha1: 3a26a72ec9de52be406ef68aed79510e15025d48
sha256: b227fcc7e8caff88b8cb349e79b11809015205bdd43a8f2f10964196444675f7
sha512:

c0fc789be5ee5b29db873ce3fe350a274c061e36b4e107af867287fe2dc050055964b15dfb0413aa76196db6fe8fb1698f80e1bffc8632637d3c6dfede9e513a

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
com.amazon.device.messaging.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.piusworks.contact.permission.RECEIVE_ADM_MESSAGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
android.permission.BLUETOOTH_ADMIN	dangerous	bluetooth administration	Allows an application to configure the local Bluetooth phone and to discover and pair with remote devices.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_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.INTERNET	dangerous	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.
com.android.vending.BILLING	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.piusworks.contact.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
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.
com.sec.android.provider.badge.permission.READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sec.android.provider.badge.permission.WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.UPDATE_SHORTCUT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonyericsson.home.permission.BROADCAST_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.anddoes.launcher.permission.UPDATE_COUNT	dangerous	Unknown permission from android reference	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.majeur.launcher.permission.UPDATE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.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.READ_APP_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.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.
me.everything.badger.permission.BADGE_COUNT_READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference

SHARED LIBRARY BINARY ANALYSIS

ISSUE	SEVERITY	DESCRIPTION	FILES
Found elf built without Position Independent Executable (PIE) flag	high	In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. Built with option <strong>-pie</strong>.	lib/mips64/libtbxml.so

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL 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>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.onesignal.BootUpReceiver) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.onesignal.UpgradeReceiver) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

ISSUE	SEVERITY	DESCRIPTION
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]	high	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.
Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
High Intent Priority (999) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	cordova/plugins/Diagnostic_Notifications.java cordova/plugins/Diagnostic_External_Storage.java cordova/plugins/Diagnostic_Camera.java cordova/plugins/Diagnostic_Wifi.java cordova/plugins/Diagnostic.java cordova/plugins/Diagnostic_Location.java cordova/plugins/Diagnostic_Bluetooth.java cordova/plugins/Diagnostic_NFC.java plugin/google/maps/PluginLocationService.java plugin/google/maps/MyPluginLayout.java plugin/google/maps/CordovaGoogleMaps.java plugin/google/maps/PluginEnvironment.java plugin/google/maps/PluginMap.java plugin/google/maps/MyPlugin.java plugin/google/maps/PluginMarkerCluster.java plugin/google/maps/AsyncLoadImage.java plugin/google/maps/PluginMarker.java bolts/MeasurementEvent.java cc/fovea/PurchasePlugin.java com/plugin/gcm/OneSignalPush.java com/plugin/gcm/OneSignalController.java com/onesignal/AndroidSupportV4Compat.java com/onesignal/JobIntentService.java com/onesignal/OneSignal.java com/onesignal/shortcutbadger/ShortcutBadger.java com/randdusing/bluetoothle/BluetoothLePlugin.java com/appfeel/cordova/admob/AdMobRewardedVideoAdListener.java com/appfeel/cordova/admob/AdMobAds.java com/appfeel/cordova/admob/AdMobAdsAdListener.java com/phonegap/plugins/barcodescanner/BarcodeScanner.java

ISSUE	SEVERITY	STANDARDS	FILES
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	cordova/plugins/Diagnostic.java com/appfeel/cordova/admob/AdMobAds.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	cordova/plugins/Diagnostic.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	plugin/google/maps/PluginLocationService.java plugin/google/maps/PluginMap.java plugin/google/maps/PluginTileProvider.java plugin/google/maps/PluginUtil.java plugin/google/maps/AsyncLoadImage.java plugin/google/maps/PluginGroundOverlay.java plugin/google/maps/PluginMarker.java de/appplant/cordova/plugin/background/BackgroundModeExt.java de/appplant/cordova/plugin/background/BackgroundMode.java com/plugin/gcm/OneSignalPush.java com/onesignal/OutcomeEvent.java com/onesignal/TrackAmazonPurchase.java com/tv/plugin/AddressImpl.java
IP Address disclosure	warning	**CVSS V2:** 4.3 (medium) **CWE:** CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor **OWASP MASVS:** MSTG-CODE-2	plugin/google/maps/PluginKmlOverlay.java plugin/google/maps/PluginTileProvider.java plugin/google/maps/AsyncLoadImage.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	bolts/MeasurementEvent.java com/plugin/gcm/OneSignalPush.java com/onesignal/PushRegistratorFCM.java com/onesignal/OneSignalNotificationManager.java com/onesignal/OneSignalRemoteParams.java com/onesignal/OSInAppMessageController.java com/onesignal/WebViewManager.java com/onesignal/NotificationBundleProcessor.java com/onesignal/GcmBroadcastReceiver.java

ISSUE	SEVERITY	STANDARDS	FILES
Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	**CVSS V2:** 8.8 (high) **CWE:** CWE-749 - Exposed Dangerous Method or Function **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-PLATFORM-7	bolts/WebViewAppLinkResolver.java com/onesignal/WebViewManager.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	nl/xservices/plugins/SocialSharing.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.java
Remote WebView debugging is enabled.	high	**CVSS V2:** 5.4 (medium) **CWE:** CWE-919 - Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/onesignal/WebViewManager.java
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.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	com/onesignal/OneSignalDbHelper.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	com/appfeel/cordova/admob/AdMobAds.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
onesignal.com	good	**IP:** 104.18.226.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
127.0.0.1	good	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.0 **Longitude:** 0.0 **View:** Google Map
api.whatsapp.com	good	**IP:** 157.240.8.53 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

🌐 URLS

URL	FILE
data:image http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/	plugin/google/maps/PluginKmlOverlay.java
http://play.google.com/store/apps/details?id=com.google.android.gms	plugin/google/maps/CordovaGoogleMaps.java
http://play.google.com/store/apps/details?id=com.google.android.gms	plugin/google/maps/PluginEnvironment.java
data:image/ data:image/png;base64, javascript:if(window.cordova){cordova.fireDocumentEvent('plugin_touch', javascript:if('%s'	plugin/google/maps/PluginMap.java
javascript:if('%s'	plugin/google/maps/PluginStreetViewPanorama.java
javascript:plugin.google.maps.Map._onOverlayEvent('	plugin/google/maps/MyPlugin.java

URL	FILE
javascript:if(window.cordova){cordova.fireDocumentEvent('%s-%s-tileoverlay', data:image/ http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/	plugin/google/maps/PluginTileProvider.java
data:image http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/ data:image/	plugin/google/maps/AsyncLoadImage.java
javascript:boltsWebViewAppLinkResolverResult.setValue((function()	bolts/WebViewAppLinkResolver.java
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
http://play.google.com/store/account/subscriptions http://play.google.com/store/paymentmethods	cc/fovea/PurchasePlugin.java
https://onesignal.com/android_frame.html	com/onesignal/OneSignalChromeTabAndroidFrame.java
data:JSON	com/onesignal/OutcomesUtils.java
https://onesignal.com/api/v1/	com/onesignal/OneSignalRestClient.java
javascript:cordova.fireDocumentEvent(admob.events.onAdLeftApplication, javascript:cordova.fireDocumentEvent(admob.events.onAdFailedToLoad, javascript:cordova.fireDocumentEvent(admob.events.onAdLoaded, javascript:cordova.fireDocumentEvent(admob.events.onAdOpened, javascript:cordova.fireDocumentEvent(admob.events.onAdRewarded, javascript:cordova.fireDocumentEvent(admob.events.onAdClosed, javascript:cordova.fireDocumentEvent(admob.events.onAdStarted, javascript:cordova.fireDocumentEvent(admob.events.onAdCompleted,	com/appfeel/cordova/admob/AdMobRewardedVideoAdListener.java
javascript:cordova.fireDocumentEvent(admob.events.onAdLoaded, javascript:cordova.fireDocumentEvent(admob.events.onAdFailedToLoad, javascript:cordova.fireDocumentEvent(admob.events.onAdOpened, javascript:cordova.fireDocumentEvent(admob.events.onAdLeftApplication, javascript:cordova.fireDocumentEvent(admob.events.onAdClosed,	com/appfeel/cordova/admob/AdMobAdsAdListener.java

✉ EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	URL
Facebook Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places	https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share	https://reports.exodus-privacy.eu.org/trackers/70
Google Ads	https://reports.exodus-privacy.eu.org/trackers/71
Google DoubleClick	https://reports.exodus-privacy.eu.org/trackers/5
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal	https://reports.exodus-privacy.eu.org/trackers/193

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

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

© 2020 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.