檔案名稱:	Cardiago.apk
檔案大小:	19.2 MB (19242922 bytes)
MD5:	71612D9134E4D91C963F9692C4C73458
SHA1:	A4C25C8182286C56AD0E06D281EA7C0D80417679
SHA256:	D43F268B0023FCA47C30A49E60CA75D4E3EDBE97FADF6542F06AB20C609AF7C0
上傳時間:	2016-07-04 16:22:47
開始分析時間:	2016-07-04 16:22:53
結束分析時間:	2016-07-04 16:30:12
Package Name :	com.iii.cardiago
App Version :	1.0
SDK Version :	14
Main Activity :	com.iii.cardiago.Welcom
加殼資訊:	未加殼

安全檢測結果:

- 工業局行動APP規範有1未通過. OWASP檢測到 5 項風險

經濟部工業局行動應用App基本資安檢測基準

編號	檢測內容	檢測結果	說明
4.1.2.3.4	行動應用程式應避免將敏感性資料儲存於暫存檔與記錄檔中	通過	-
4.1.2.3.5	敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理在儲存	不通過	儲存前未加密
4.1.2.3.6	敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取	通過	-
4.1.2.3.7	敏感性資料應避免出現於行動應用程式之程式碼	通過	-
4.1.5.1.1	行動應用程式應避免含有惡意程式碼	通過	-

經濟部工業局行動應用App基本資安檢測結果相關資訊

4.1.2.3.5 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理在儲存

+ 證據 - 1

儲存前未加密

@ apk/smali/org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.smali

line#1234 invoke-virtual v1 v3 Ljava/io/FileOutputStream;->write([B)V

@ apk/smali/cz/msebera/android/httpclient/impl/client/cache/FileResourceFactory.smali

line#244 invoke-virtual v3 v0 v6 v2 Ljava/io/FileOutputStream;->write([BII)V

@ apk/smali/com/google/android/gms/tagmanager/zzcn.smali

line#243 invoke-virtual v2 v3 Ljava/io/FileOutputStream;->write([B)V

OWASP/CVE行動應用風險

OWASP-M2 **此行動應用程式使用了不安全的資料儲存機制，有被他人竊取的風險。**

- OWASP-M2-1 此行動應用程式未使用安全的加密寫入機制，有造成資料外洩之潛在風險

@ apk/smali/org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.smali

line#1234 invoke-virtual v1 v3 Ljava/io/FileOutputStream;->write([B)V

@ apk/smali/cz/msebera/android/httpclient/impl/client/cache/FileResourceFactory.smali

line#244 invoke-virtual v3 v0 v6 v2 Ljava/io/FileOutputStream;->write([BII)V

@ apk/smali/com/google/android/gms/tagmanager/zzcn.smali

line#243 invoke-virtual v2 v3 Ljava/io/FileOutputStream;->write([B)V

OWASP-M4 **此行動應用程式使用了不安全的資料存取機制，有可能在存取的過程被他人竊取的風險。**

- OWASP-M4-6 此應用程式存在有不安全的資料儲存設定，可以被其他程式讀取資料，有成資料外洩之潛在風險

@ apk/smali/com/google/android/gms/internal/zzar.smali

line#28 invoke-virtual p1 v0 v1 Landroid/content/Context;->getSharedPreferences(Ljava/lang/String;I)

line#26 const/4 v1 0x1

OWASP-M6 **此行動應用程式使用了不安全的加密機制，有被他人破解的風險。**

- OWASP-M6-4 此應用程式在建置加密物件時，使用了加密模式「ECB」參數，該參數在加密使用上較為不安全

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.smali

line#1018 invoke-static v11 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#1016 const-string v11 DES/ECB/NoPadding

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.smali

line#1155 invoke-static v10 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#1153 const-string v10 DES/ECB/NoPadding

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl$CipherGen.smali

line#598 invoke-static v8 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#596 const-string v8 DES/ECB/NoPadding

- OWASP-M6-5 此應用程式使用了弱加密演算法

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.smali

line#1018 invoke-static v11 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#1016 const-string v11 DES/ECB/NoPadding

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.smali

line#1155 invoke-static v10 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#1153 const-string v10 DES/ECB/NoPadding

@ apk/smali/cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl$CipherGen.smali

line#598 invoke-static v8 Ljavax/crypto/Cipher;->getInstance(Ljava/lang/String;)Ljavax/crypto/Cipher;

line#596 const-string v8 DES/ECB/NoPadding

OWASP-M10	此行動應用程式未有安全的程式碼保護，有被惡意竄改的潛在風險

- 未加殼

防毒軟體檢測結果

ClamAV	未檢測出可疑檔案

憑證資訊

擁有者:	CN=Android Debug O=Android C=US
發行者:	CN=Android Debug O=Android C=US
序號:	1b4595d5
有效期間:	Thu May 05 16:47:43 CST 2016 ~ Sat Apr 28 16:47:43 CST 2046
MD5:	09:67:0E:D4:B1:E2:64:78:89:84:F9:5E:9D:43:D8:D9
SHA1:	EC:8B:B4:E7:44:0B:BC:B3:4B:D6:21:57:F2:F3:8C:E8:17:B1:F5:AD
SHA256:	C6:DF:E6:D7:BD:0A:98:F3:EB:7B:B5:0C:8F:3C:F8:0B:98:EB:6C:66:8A:0A:3E:AE:40:F5:68:A1:D1:01:35:E4
簽章演算法:	SHA256withRSA
版本:	3

APP 使用之權限列表

位置

概略位置

精確位置

網路

查看網路連線

開啟網路連線

通訊

與藍牙裝置配對

	搜尋、配對藍芽裝置
電話	
	直接撥打電話號碼
相機	
	拍攝相片和影片
其他	
	禁用鍵盤鎖
	讀取系統紀錄檔
	控制震動
	防止裝置進入休眠狀態
麥克風	
	錄製音訊
儲存空間	
	寫入USB 儲存裝置的內容

APP 活動(Activity)列表

.Welcom	@android:exported = false
Main	@android:exported = false
FirstLayout	@android:exported = false
Parking	@android:exported = false
ConvenientInfo	@android:exported = false
GoodThing	@android:exported = false
RegistrationActivity	@android:exported = false
iii.obdcar.car_diago_plus.WelComeActivity	@android:exported = false
iii.obdcar.car_diago_plus.RegistrationActivity	@android:exported = false
iii.obdcar.car_diago_plus.MenuActivity	@android:exported = false
com.facebook.LoginActivity	@android:exported = false
iii.obdcar.car_trip.TakePicture	@android:exported = false
iii.obdcar.realtime_info.RealTimeCarInfo	@android:exported = false
iii.obdcar.car_trip.CarTrips	@android:exported = false
iii.obdcar.car_diago_plus.CarDiagnosis	@android:exported = false
iii.obdcar.car_diago_plus.Setting	@android:exported = false
iii.obdcar.car_diago_plus.UpdateUserData	@android:exported = false
iii.obdcar.car_trip.CarTripShow	@android:exported = false
iii.obdcar.roadmap.RoadMapMenu	@android:exported = false
iii.obdcar.vehicle_trouble_recall.ListActivity	@android:exported = false
iii.obdcar.vehicle_trouble_recall.ProblemActivity	@android:exported = false

iii.obdcar.vehicle_trouble_recall.ProblemSetActivity	@android:exported = false
iii.obdcar.vehicle_trouble_recall.SolutionActivity	@android:exported = false
iii.obdcar.vehicle_trouble_recall.SublistActivity	@android:exported = false
iii.obdcar.broadcast.ObdBroadcastDialog	@android:exported = false
iii.obdcar.broadcast.ObdBroadcastRankDialog	@android:exported = false
iii.obdcar.broadcast.ObdBroadcastTemperatrueDialog	@android:exported = false
iii.obdcar.car_diago_plus.EmailConfirmActivity	@android:exported = false
iii.obdcar.car_diago_plus.LookPhotoActivity	@android:exported = false
com.openlife.checkme.CheckmeActivity	@android:exported = false
com.openlife.checkme.main.CheckmeMainActivity	@android:exported = false
com.openlife.checkme.map.MapActivity	@android:exported = false
com.zxing.CaptureActivity	@android:exported = false
com.openlife.checkme.ui.ManualActivity	@android:exported = false
com.openlife.checkme.exchange.MobileCertificationActivity	@android:exported = false
com.openlife.checkme.exchange.MobileConfirmActivity	@android:exported = false
com.openlife.checkme.main.GameActivity	@android:exported = false
com.facebook.FacebookActivity	@android:exported = false

APP 服務(Service)列表

iii.obdcar.obd_service.ObdService	@android:exported = false
org.altbeacon.beacon.service.BeaconService	@android:exported = false
org.altbeacon.beacon.BeaconIntentProcessor	@android:exported = false

APP 接收器(Receiver)列表

iii.obdcar.bluetooth_pair.BluetoothConnectActivityReceiver	@android:exported = false
iii.obdcar.broadcast.ObdBroadcastReceiver	@android:exported = false
org.altbeacon.beacon.startup.StartupBroadcastReceiver	@android:exported = false

APP 提供器(Provider)列表

N/A

APP使用第三方函式庫

- 函式庫檔案 :

  N/A

- 第三方函式之函式呼叫 :

  apk/smali/com/facebook/internal/FragmentWrapper.smali:7:.field private nativeFragment:Landroid/app/Fragment;