4G 應用程式 App 基本資安檢測複測結果合格廠商名單

編號	App 名稱	作業系統	通過版本
1	國泰人壽	Android	4.0.8
2	南山人壽行動智慧網	Android	2.26.1
3	三商美邦人壽行動夥伴	iOS	1.1
4	歐付寶行動支付	iOS	2.13.0.14
5	Hami Wallet 中華電信行動通信分公司	Android	2.17.20121505
6	遠傳行動客服	Android	3.7.2
7	台灣大哥大行動客服	Andoid	7.8.3

4G 應用程式 App 基本資安檢測複測結果(不合格項目)彙整表

項次	級別	檢測編號	檢測項目	不符合 App 數量
1	中級	4.1.1.1.2.	應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途	0
2	中級	4.1.1.3.1.	開發者應提供回報安全性問題之管道	0
3	中級	4.1.2.1.1.	應於蒐集敏感性資料前，取得使用者同意	2
4	中級	4.1.2.1.2.	應提供使用者拒絕蒐集敏感性資料之權利	2
5	中級	4.1.2.3.1.	應於儲存敏感性資料前，取得使用者同意	1
6	中級	4.1.2.3.2.	應提供使用者拒絕儲存敏感性資料之權利	0
7	初級	4.1.2.3.4.	應避免將敏感性資料儲存於暫存檔或紀錄檔中	6
8	初級	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，進行加密處理再儲存	8
9	初級	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	0
10	初級	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	1
11	中級	4.1.2.4.1.	透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密	0
12	中級	4.1.2.5.1.	行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意	0
13	中級	4.1.2.5.2.	應提供使用者拒絕分享敏感性資料之權利	0
14	中級	4.1.2.5.3.	分享敏感性資料時，應避免未授權之行動應用程式存取	0
15	高級	4.1.3.1.1.	應於使用付費資源前主動通知使用者	0
16	高級	4.1.3.1.2.	應提供使用者拒絕使用付費資源之權利	0
17	高級	4.1.3.2.1.	應於使用付費資源前進行使用者認證	4
18	高級	4.1.3.2.2.	應記錄使用之付費資源與時間	0
19	中級	4.1.4.1.1.	應有適當之身分認證機制，確認使用者身分	2
20	中級	4.1.4.1.2.	應依使用者身分授權	2
21	中級	4.1.4.2.1.	應避免使用具有規則性之交談識別碼	0
22	中級	4.1.4.2.2.	應確認伺服器憑證之有效性	2

23	中級	4.1.4.2.3.	應確認伺服器憑證為可信任之憑證機構、政府機關或企業簽發	0
24	中級	4.1.4.2.4.	應避免與未具有效憑證之伺服器，進行連線與傳輸資料	1
25	初級	4.1.5.1.1.	應避免含有惡意程式碼	2
26	中級	4.1.5.1.2.	應避免資訊安全漏洞	9
27	中級	4.1.5.3.1.	於引用之函式庫有更新時，應備妥對應之更新版本	0
28	初級	4.1.5.4.1.	應針對使用者輸入之字串，進行安全檢查	5
29	中級	4.1.5.4.2.	應提供相關注入攻擊防護機制	0