

審案實務分享：提升送審案件品質與技術一致性探討

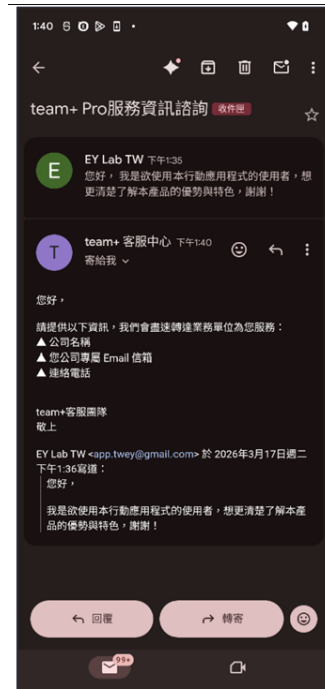
行動應用資安聯盟 技術專家

We are Team MAS



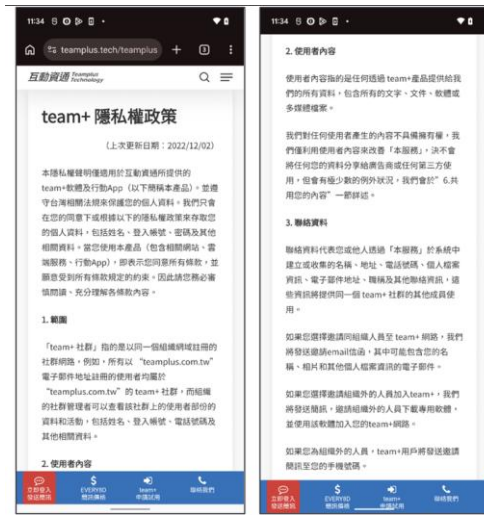
4.1.1.3.1 檢測結果說明-建議修正

- 若行動應用程式已發布，檢查行動應用程式是否於應用程式商店 或行動應用程式內，提供聯絡網頁、留言板、電子郵件、電話或其他類型聯絡方式，並經測試可實際聯絡成功。若行動應用程式尚未發布，檢查調查表內是否有說明預計提供回報安全性問題之管道與聯絡方式，並經測試可實際聯絡成功。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- **建議修正原因：佐證資料時間點一樣**



4.1.2.3.2 檢測結果說明-不通過

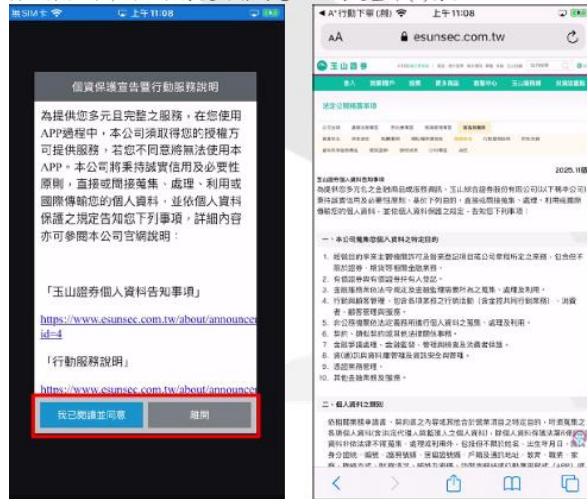
- 行動應用程式提供使用者拒絕儲存敏感性資料之功能，且在使用者拒絕敏感性資料儲存的情況下，行動應用程式未檢出儲存敏感性資料。
- **不通過原因：所提供之佐證資料僅可符合4.1.2.3.1(若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。)**



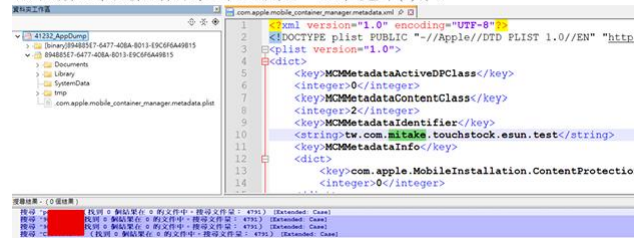
4.1.2.3.2 檢測結果說明-可參考

檢測工具：人工檢視、notepad++

經檢查，行動應用程式確實於應用程式內皆有提供個人資料使用條款，所有儲存之敏感性資料於條款內聲明及取得使用者同意，故判定基準(1)符合。



經檢查，應用程式於使用者拒絕儲存敏感性資料情境下，未將個人資料、帳號、密碼、生物辨識資訊等敏感性資料寫入本地儲存區，故判定基準(2)符合。



4.1.2.3.5 檢測結果說明-不通過

4.1.2.3.5 行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中

■ 檢測分類：L3

■ 檢測基準：

(1) 檢查行動應用程式是否未檢出將敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準

(2) 檢查行動應用程式是否未檢出將敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準

(3) 檢查行動應用程式是否將敏感性資料儲存於冗餘檔案或日誌檔案且已用安全加密函式保護。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準

■ 檢測結果：

符合要求：符合所有檢測基準 或行動應用程式未檢出儲存敏感性資料

不符合要求：任一檢測基準不符合

行動應用App基本資安檢測基準-4.1.2.3.5

4.1.2.3.5. 行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中

檢測編號	4.1.2.3.5
檢測項目	行動應用程式冗餘檔案或日誌檔案敏感性資料儲存限制
檢測分類	L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-STORAGE-2
技術要求	行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中
檢測基準	(1) 檢查行動應用程式是否未檢出將敏感性資料儲存於冗餘檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(2) 檢查行動應用程式是否未檢出將敏感性資料儲存於日誌檔案。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
	(3) 檢查行動應用程式是否將敏感性資料儲存於冗餘檔案或日誌檔案且已用安全加密函式保護。如為「是」則符合本項檢測基準； 「否」則不符合本項檢測基準。
檢測結果	符合要求：檢測基準(1)、(2)皆符合或符合檢測基準(3)。 不符合要求：檢測基準(1)或(2)不符合且檢測基準(3)不符合。
備註	根據美國國家標準技術研究院建議：於 2023 年 12 月 31 日以後不允許對 Triple DES (3DES、DES3) 加密之支援。故將 3DES 加密從基準中剔除。

4.1.2.3.6 檢測結果說明-不通過(2/2)

- 檢查行動應用程式所使用之加密函式之金鑰是否僅採用符合ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators)至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- **不通過原因：無法證明符合標準**

測試人員檢視動態分析結果，觀測到行動應用程式多次呼叫 java.security.SecureRandom 產生金鑰所需之隨機位元組，在 Android 系統中，SecureRandom 會調用作業系統提供的安全亂數來源，屬於符合國際安全標準要求的安全亂數生成方式，因此符合此項檢測基準。

```
java.security.SecureRandom called
Generated bytes: -112,68,-13,-122,-64,-39,13,-13,-119,-46,-68,119,-93,89,41,97
java.security.SecureRandom called
Generated bytes: -31,-36,51,32,-99,126,31,-37,-75,11,-102,50,-116,67,-64,-9
java.security.SecureRandom called
Generated bytes: -53,92,-101,16,-76,-7,-66,103,-82,-31,-114,-35,75,-109,0,-90
java.security.SecureRandom called
Generated bytes: -106,-13,-51,24,-17,-81,113,68,-124,-79,-117,-105,-116,11,107,72
java.security.SecureRandom called
Generated bytes: 120,1,17,98,-65,-69,79,95,1,14,52,-121,3,33,-36,81
java.security.SecureRandom called
Generated bytes: 112,21,-102,-107,-100,-23,127,-100,15,96,35,60,-45,-86,-81,75
```

經檢測，行動應用程式有對安全敏感性資料進行加密儲存，採用 AES 加密演算法且金鑰長度符合 128bit 以上要求。金鑰產生過程採用 SecureRandom 作為亂數產生函式，該函式於 Android 平台未指定 Provider 時，預設由 Conscrypt Provider 實作，其底層採用 Google BoringSSL/BoringCrypto 函式庫，已通過 NIST CMVP FIPS 140-2 驗證 (Certificate #3753)。BoringCrypto 採用符合 NIST SP 800-90A 規範之 CTR-DRBG 作為系統所有亂數輸出之主要介面 (RAND_bytes)，包含 SecureRandom 在內之所有亂數需求均透過此機制產生，故判定符合。

```
if (provider != null) {
    try {
        secureRandom = SecureRandom.getInstance("SHA1PRNG", provider);
    } catch (GeneralSecurityException unused) {
    }
} else {
    try {
        provider2 = (Provider) Class.forName("org.conscrypt.Conscrypt").getMethod("newProvider", null).invoke(null, null);
    } catch (Throwable unused2) {
    }
    if (provider2 != null) {
        try {
            secureRandom = SecureRandom.getInstance("SHA1PRNG", provider2);
        } catch (GeneralSecurityException unused3) {
        }
    } else {
        secureRandom = new SecureRandom();
    }
}
secureRandom.nextLong();
return secureRandom;
}
```

4.1.2.3.6 檢測結果說明-可參考(1/3)

- 檢查行動應用程式之非冗餘檔案及非日誌檔案內之敏感性資料是否僅採用金鑰有效長度為 128 位元 (含) 以上之先進加密標準 (AES)，或使用 ChaCha20。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

MitakeJni.c 程式碼 使用 AES_CBC_ENCRYPE 進行文字加密

```
/**
 * AES cbc模式 加密用
 * c1 有用
 * c2 沒用
 */
JNIEXPORT jbyteArray JNICALL Java_com_mitake_jni_MitakeJni_c(
    JNIEnv *env, jclass jcl, jbyteArray c1, jbyteArray c2)
{
    //LOGI("%s", __FUNCTION__);
    jbyteArray OutData;

    if (c1)
    {
        int InDataLen = (int) (*env)->GetArrayLength(env, c1);

        if (InDataLen > 0)
        {
            /* 計算加密後的資料長度 */
            int ResDataLen = AES_BLOCK_SIZE;
            if (InDataLen >= AES_BLOCK_SIZE)
                ResDataLen = ((int) ((double) InDataLen / (double) AES_BLOCK_SIZE + 1) * );

            unsigned char *InDataPadding = malloc(ResDataLen + 1);
            InDataPadding[ResDataLen] = '\0';
            unsigned char *ResData = malloc(ResDataLen + 1);
            ResData[ResDataLen] = '\0';

            /* 拷貝 輸入資料, java_mem to c_mem */
            (*env)->GetByteArrayRegion(env, c1, 0, InDataLen, (jbyte *) InDataPadding);

            /* 填充, 固定填充0x10 */
            memset(InDataPadding + InDataLen, 0x10, ResDataLen - InDataLen);

            /* 加密 */
            AES_CBC_ENCRYPT(InDataPadding, ResData, ResDataLen, NULL, NULL, 256);
        }
    }
}
```

4.1.2.3.6 檢測結果說明-可參考(2/3)

- 檢查行動應用程式所使用之加密函式之金鑰是否僅採用符合ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators)至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

使用 NIST 所提供的亂數檢測工具(sts-2.1.2)對 SecureRandom 進行檢測，經檢測符合 NIST SP 800-22。

使用 SecureRandom 生成亂數

```
securerandom.java x
1 import java.io.FileOutputStream;
2 import java.security.SecureRandom;
3
4 public class SecureRandomTestData {
5     public static void main(String[] args) throws Exception {
6         SecureRandom sr = new SecureRandom();
7         byte[] randomBytes = new byte[20 * 1024 * 1024]; // 20MB
8         sr.nextBytes(randomBytes);
9
10        try (FileOutputStream fos = new FileOutputStream("randomData20.bin")) {
11            fos.write(randomBytes);
12        }
13        System.out.println("Generated 20MB of random data for testing.");
14    }
15 }
16 }
```

行動應用程式使用SecRandomCopyBytes亂數函式。

```
> rabin2 -zzq MRSF.UAT | grep -i "SecRandom"
0x100169b79 _SecRandomCopyBytes
0x10016a3ec _SecRandomDefault
0x10018f112 _SecRandomCopyBytes
0x10018fee4 _SecRandomDefault
```

使用NIST所提供的亂數檢測工具(sts-2.1.2)對 SecRandomCopyBytes 進行檢測，經檢測符合 NIST SP 800-22。

```
Parameter Adjustments
[1] Block Frequency Test - block length(M): 128
[2] NonOverlapping Template Test - block length(m): 9
[3] Overlapping Template Test - block length(m): 9
[4] Approximate Entropy Test - block length(m): 10
[5] Serial Test - block length(M): 16
[6] Linear Complexity Test - block length(M): 500

Select Test (0 to continue): 0
How many bitstreams? 20

Input File Format:
[0] ASCII - A sequence of ASCII 0's and 1's
[1] Binary - Each byte in data file contains 8 bits of data

Select input mode: 1

Statistical Testing In Progress.....
Statistical Testing Complete!!!!!!!!!!!!
```

檢測結果SecRandomCopyBytes符合NIST SP 800-22

4.1.2.3.6 檢測結果說明-可供參考(3/3)

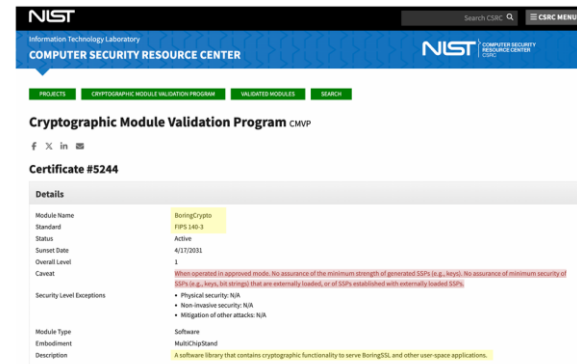
- 檢查行動應用程式所使用之加密函式之金鑰是否僅採用符合ANSI X9.17、FIPS 140-3、NIST SP 800-22 及 SP 800-90A (CAVP Testing: Random Number Generators)至少其中一項之安全的亂數產生函式。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

經檢視開發商提供的程式碼片段，確認行動應用程式使用 SecureRandom 產生金鑰所需之亂數。

附錄 B：AES 金鑰與 IV 產生

```
private void genAESKey() throws Exception {  
    // 1. 使用 CSPRNG 產生 128-bit AES 金鑰  
    byte[] aesKey = new byte[16];  
    SecureRandom secureRandom = new SecureRandom();  
    secureRandom.nextBytes(aesKey);  
  
    // 2. 使用 CSPRNG 產生 12-byte GCM IV，Base64 編碼後存入 SharedPreferences  
    byte[] generated = secureRandom.generateSeed(12);  
    String iv = Base64.encodeToString(generated, Base64.DEFAULT);  
    prefsHelper.setIV(iv); // → 寫入 PREF_KEY_IV  
  
    // 3. AES 金鑰以 KeyStore 中的 RSA 公鑰加密後，存入 SharedPreferences  
    String encryptAESKey = encryptRSA(aesKey);  
    prefsHelper.setAESKey(encryptAESKey); // → 寫入 PREF_KEY_AES  
}
```

依據 NIST Cryptographic Module Validation Program (CMVP) Certificate #5244，BoringCrypto 已通過 FIPS 140-3 驗證。另 Android 預設 Security Provider (Conscrypt) 之 cryptographic backend 採用 BoringSSL 實作，因此可確認測試標的所使用之亂數生成機制係建立於具備現代密碼學安全設計之 cryptographic implementation 上，因此符合此項檢測基準。



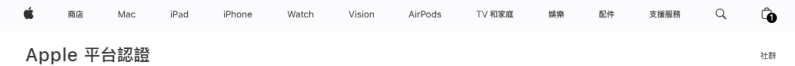
NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PRODUCTS | CRYPTOGRAPHIC MODULE VALIDATION PROGRAM | VALIDATED MODULES | STANDARDS

Cryptographic Module Validation Program CMVP

Certificate #5244

Details	
Module Name	BoringCrypto
Standard	FIPS 140-3
Status	Active
Summit Date	4/17/2021
Overall Level	1
Comment	When operated in approved mode, No assurance of the minimum strength of generated SP800-31a, key(s). No assurance of minimum security of SP800-31a, key(s) (strings) that are externally loaded, or of SP800-31a established with externally loaded SP800-31a, key(s).
Security Level Exceptions	<ul style="list-style-type: none">Physical security: N/ANon-reversible security: N/AMitigation of other attacks: N/A
Module Type	Software
Embedment	Multi-Chip/Board
Description	A software library that contains cryptographic functionality to serve BoringSSL and other open source applications.



Apple 平台認證

在手中搜尋

目錄

關於 Apple 安全性認證

Apple 維護安全認證計畫，以符合全球對安全性保障的要求。

從認證基本要件開始著手，這些基本要件可在適用情況下跨多個平台廣泛應用，其中一個基本要件就是 [CoreCrypto](#) 的認證，其用於 Apple 所開發作業系統內的軟體體加密編譯模組開發。第二個基本要件是 [安全隔離區](#)（內嵌在許多 Apple 裝置內）的認證，第三個則是 [Secure Element \(SE\)](#) 的認證，應用於配備 Face ID 和 Touch ID 的 Apple 裝置。這些硬體認證基本要件為更廣泛的平台安全性認證形成了基礎。

Apple 以這些核心安全性功能認證的為基礎，為作業系統、應用程式和安全性相關的功能（例如嚴格驗證機制）的進一步認證奠定了基礎。

加密編譯演算法驗證

驗證許多加密編譯演算法和相關安全性功能的導入正確性，是 FIPS 140-3 驗證和支援其他認證的先決條件。驗證由美國國家標準暨技術研究院 (NIST) [加密編譯演算法驗證計畫 \(CAVP\)](#) 管理，你可使用 [CAVP 搜尋](#) 工具來找到 Apple 導入的驗證憑證。如需更多資訊，請參閱 [加密編譯演算法驗證計畫 \(CAVP\) 網站](#)。

加密編譯模組驗證：FIPS 140-2/3 (ISO/IEC 19790)

自 2012 年起，每個主要作業系統發佈後，「[加密編譯模組驗證計畫 \(CMVP\)](#)」都會反覆驗證 Apple 的 [加密編譯模組](#) 是否符合加密編譯模組的「美國聯邦資訊處理標準」(FIPS 140-2)。每次發行主要版本後，Apple 都會向 CMVP 提交模組，以驗證是否符合標準。這些模組不僅可以由 Apple 作業系統使用，還以為 Apple 提供的服務提供加密編譯功能，並且可供第三方 App 使用。

4.1.2.3.11 檢測結果說明-不通過

- 檢查行動應用程式是否在輸入敏感性資料欄位中將鍵盤快取機制關閉：檢查行動應用程式於使用者輸入敏感性資料時，是否未自動修正且未帶入可能字串。如為「是」則符合檢測基準；「否」則不符合本項檢測基準。檢測結果 符合要求：符合檢測基準，或行動應用程式未檢出蒐集敏感性資料
- **不通過原因：所檢附之佐證資料皆有遮蔽，無法顯示是否未自動修正且未帶入可能字串。**

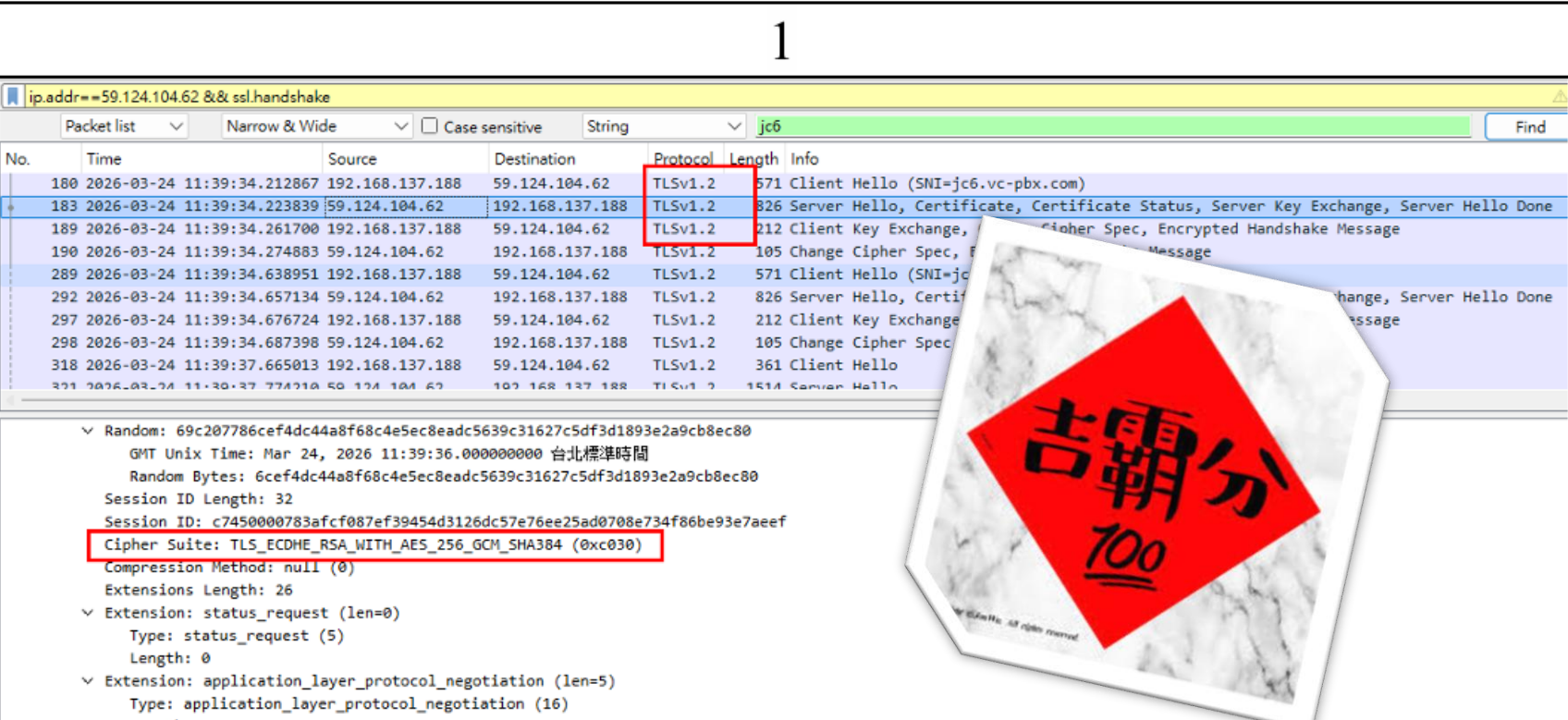


4.1.2.3.11 檢測結果說明-可參考



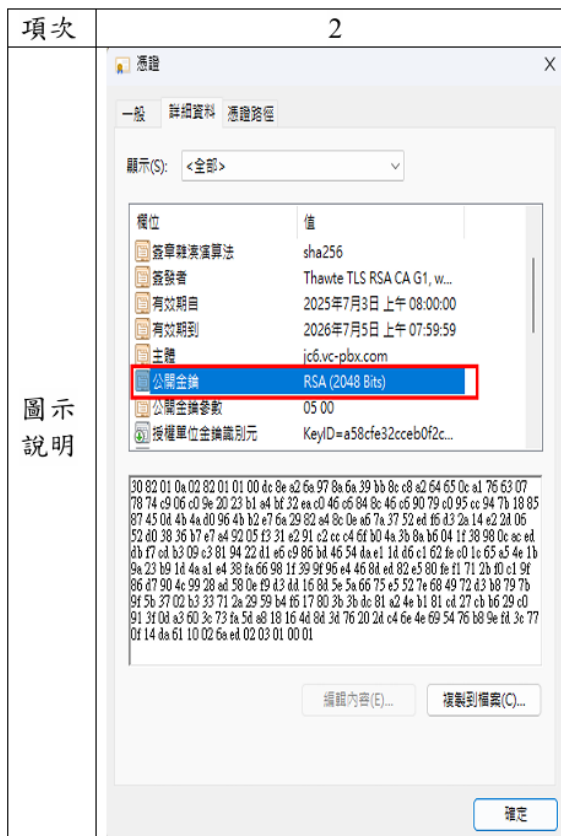
4.1.2.4.1. 檢測結果說明-可參考(1/3)

1. 行動應用程式僅採用 TLS 1.2（含）以上版本 加密協定傳輸資料，如本項檢測結果截圖說明之 項次1所示。符合基準

項次	1
圖示說明	

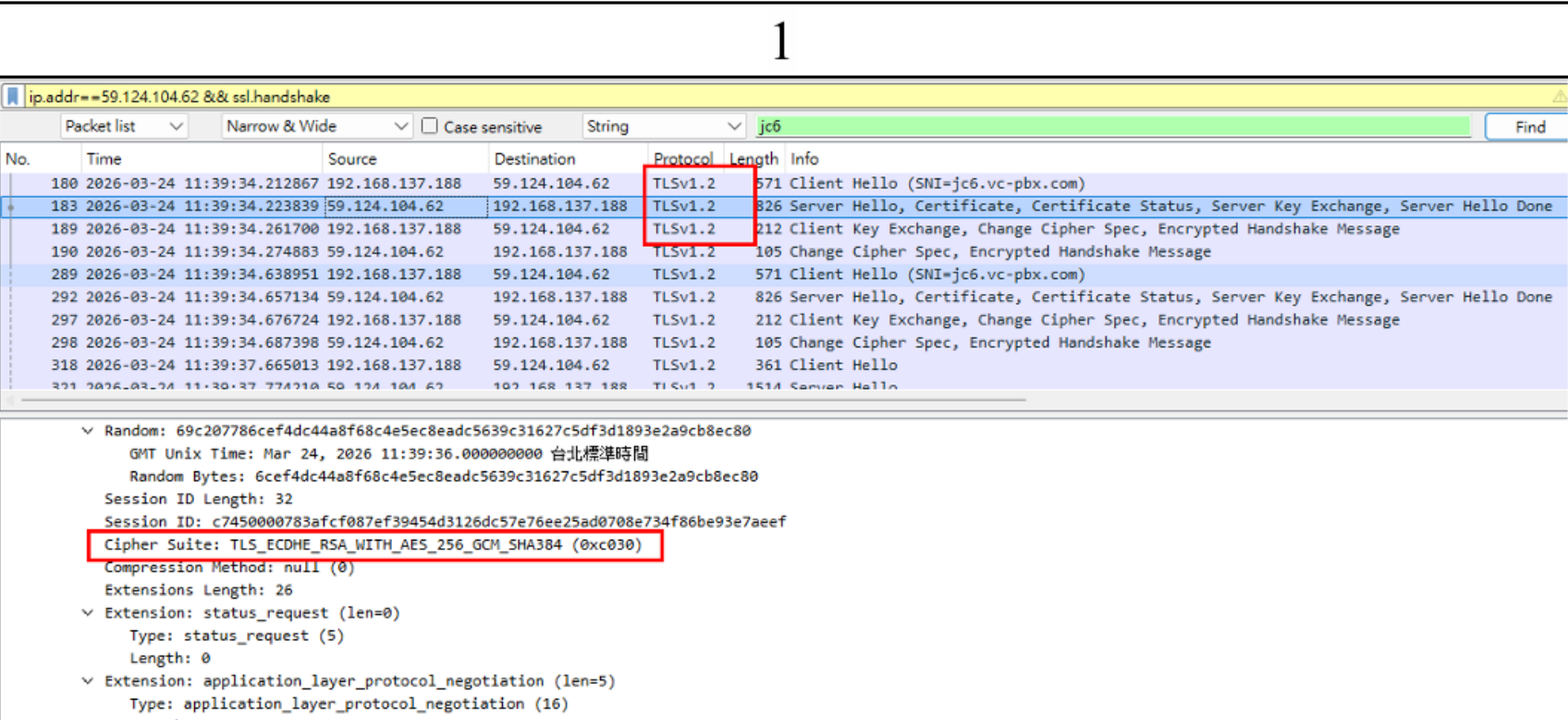
4.1.2.4.1. 檢測結果說明-可參考(2/3)

2. 行動應用程式僅採用金鑰有效長度為 2048 位元（含）以上之 RSA 加密演算法，如本項檢測結果截圖說明之項次2所示。符合基準



4.1.2.4.1. 檢測結果說明-可參考(3/3)

3. 行動應用程式僅採用金鑰有效長度為 128 位元（含）以上之進階加密標準（AES），如本項檢測結果截圖說明之項次1所示。

項次	1																																																																						
圖示說明	 <p>The screenshot shows a Wireshark capture of a TLS handshake. The packet list table is as follows:</p> <table border="1"><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>180</td><td>2026-03-24 11:39:34.212867</td><td>192.168.137.188</td><td>59.124.104.62</td><td>TLSv1.2</td><td>571</td><td>Client Hello (SNI=jc6.vc-pbx.com)</td></tr><tr><td>183</td><td>2026-03-24 11:39:34.223839</td><td>59.124.104.62</td><td>192.168.137.188</td><td>TLSv1.2</td><td>826</td><td>Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done</td></tr><tr><td>189</td><td>2026-03-24 11:39:34.261700</td><td>192.168.137.188</td><td>59.124.104.62</td><td>TLSv1.2</td><td>212</td><td>Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message</td></tr><tr><td>190</td><td>2026-03-24 11:39:34.274883</td><td>59.124.104.62</td><td>192.168.137.188</td><td>TLSv1.2</td><td>105</td><td>Change Cipher Spec, Encrypted Handshake Message</td></tr><tr><td>289</td><td>2026-03-24 11:39:34.638951</td><td>192.168.137.188</td><td>59.124.104.62</td><td>TLSv1.2</td><td>571</td><td>Client Hello (SNI=jc6.vc-pbx.com)</td></tr><tr><td>292</td><td>2026-03-24 11:39:34.657134</td><td>59.124.104.62</td><td>192.168.137.188</td><td>TLSv1.2</td><td>826</td><td>Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done</td></tr><tr><td>297</td><td>2026-03-24 11:39:34.676724</td><td>192.168.137.188</td><td>59.124.104.62</td><td>TLSv1.2</td><td>212</td><td>Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message</td></tr><tr><td>298</td><td>2026-03-24 11:39:34.687398</td><td>59.124.104.62</td><td>192.168.137.188</td><td>TLSv1.2</td><td>105</td><td>Change Cipher Spec, Encrypted Handshake Message</td></tr><tr><td>318</td><td>2026-03-24 11:39:37.665013</td><td>192.168.137.188</td><td>59.124.104.62</td><td>TLSv1.2</td><td>361</td><td>Client Hello</td></tr></tbody></table> <p>The details pane shows the following information for the selected packet:</p> <ul style="list-style-type: none">Random: 69c207786cef4dc44a8f68c4e5ec8eadc5639c31627c5df3d1893e2a9cb8ec80GMT Unix Time: Mar 24, 2026 11:39:36.000000000 台北標準時間Random Bytes: 6cef4dc44a8f68c4e5ec8eadc5639c31627c5df3d1893e2a9cb8ec80Session ID Length: 32Session ID: c7450000783afc087ef39454d3126dc57e76ee25ad0708e734f86be93e7aeefCipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)Compression Method: null (0)Extensions Length: 26Extension: status_request (len=0)<ul style="list-style-type: none">Type: status_request (5)Length: 0Extension: application_layer_protocol_negotiation (len=5)<ul style="list-style-type: none">Type: application_layer_protocol_negotiation (16)Length: 5	No.	Time	Source	Destination	Protocol	Length	Info	180	2026-03-24 11:39:34.212867	192.168.137.188	59.124.104.62	TLSv1.2	571	Client Hello (SNI=jc6.vc-pbx.com)	183	2026-03-24 11:39:34.223839	59.124.104.62	192.168.137.188	TLSv1.2	826	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done	189	2026-03-24 11:39:34.261700	192.168.137.188	59.124.104.62	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	190	2026-03-24 11:39:34.274883	59.124.104.62	192.168.137.188	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message	289	2026-03-24 11:39:34.638951	192.168.137.188	59.124.104.62	TLSv1.2	571	Client Hello (SNI=jc6.vc-pbx.com)	292	2026-03-24 11:39:34.657134	59.124.104.62	192.168.137.188	TLSv1.2	826	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done	297	2026-03-24 11:39:34.676724	192.168.137.188	59.124.104.62	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	298	2026-03-24 11:39:34.687398	59.124.104.62	192.168.137.188	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message	318	2026-03-24 11:39:37.665013	192.168.137.188	59.124.104.62	TLSv1.2	361	Client Hello
	No.	Time	Source	Destination	Protocol	Length	Info																																																																
180	2026-03-24 11:39:34.212867	192.168.137.188	59.124.104.62	TLSv1.2	571	Client Hello (SNI=jc6.vc-pbx.com)																																																																	
183	2026-03-24 11:39:34.223839	59.124.104.62	192.168.137.188	TLSv1.2	826	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done																																																																	
189	2026-03-24 11:39:34.261700	192.168.137.188	59.124.104.62	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message																																																																	
190	2026-03-24 11:39:34.274883	59.124.104.62	192.168.137.188	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message																																																																	
289	2026-03-24 11:39:34.638951	192.168.137.188	59.124.104.62	TLSv1.2	571	Client Hello (SNI=jc6.vc-pbx.com)																																																																	
292	2026-03-24 11:39:34.657134	59.124.104.62	192.168.137.188	TLSv1.2	826	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done																																																																	
297	2026-03-24 11:39:34.676724	192.168.137.188	59.124.104.62	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message																																																																	
298	2026-03-24 11:39:34.687398	59.124.104.62	192.168.137.188	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message																																																																	
318	2026-03-24 11:39:37.665013	192.168.137.188	59.124.104.62	TLSv1.2	361	Client Hello																																																																	

4.1.2.5.2. 檢測結果說明-不通過

- (2) 檢查在使用者拒絕敏感性資料分享的情況下，行動應用程式是否未分享敏感性資料。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- **不通過原因：所提供之佐證資料僅可符合4.1.2.5.1(若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。)**

行動裝置內之不同行動應用程式間，分享安全敏感性資料前，有於行動應用程式內或可信任之應用程式商店聲明，有提供不同意之選項，但使用本服務則視同取得使用者同意。



4.1.2.5.2. 檢測結果說明-可參考

檢測工具：人工檢視、iTunes

經檢查，行動應用程式「玉山證券『A+行動下單』」未發現分享敏感性資料，故判定此項符合。

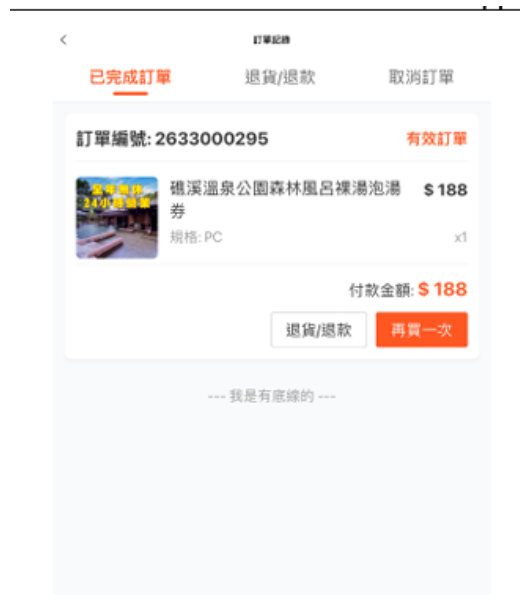
檔案共享

下列的 App 可在你的 iPhone 與這部電腦之間傳輸文件。



4.1.3.2.2 檢測結果說明-不通過

- 檢查行動應用程式於交易後，是否提供查詢交易記錄之管道，且交易記錄至少包含交易商品名稱、交易時間及交易金額之記錄。如為「是」則符合檢測基準；「否」則不符合檢測基準。
- **不通過原因：所提供之佐證資料沒有包括交易時間**



4.1.3.2.2 檢測結果說明-可參考



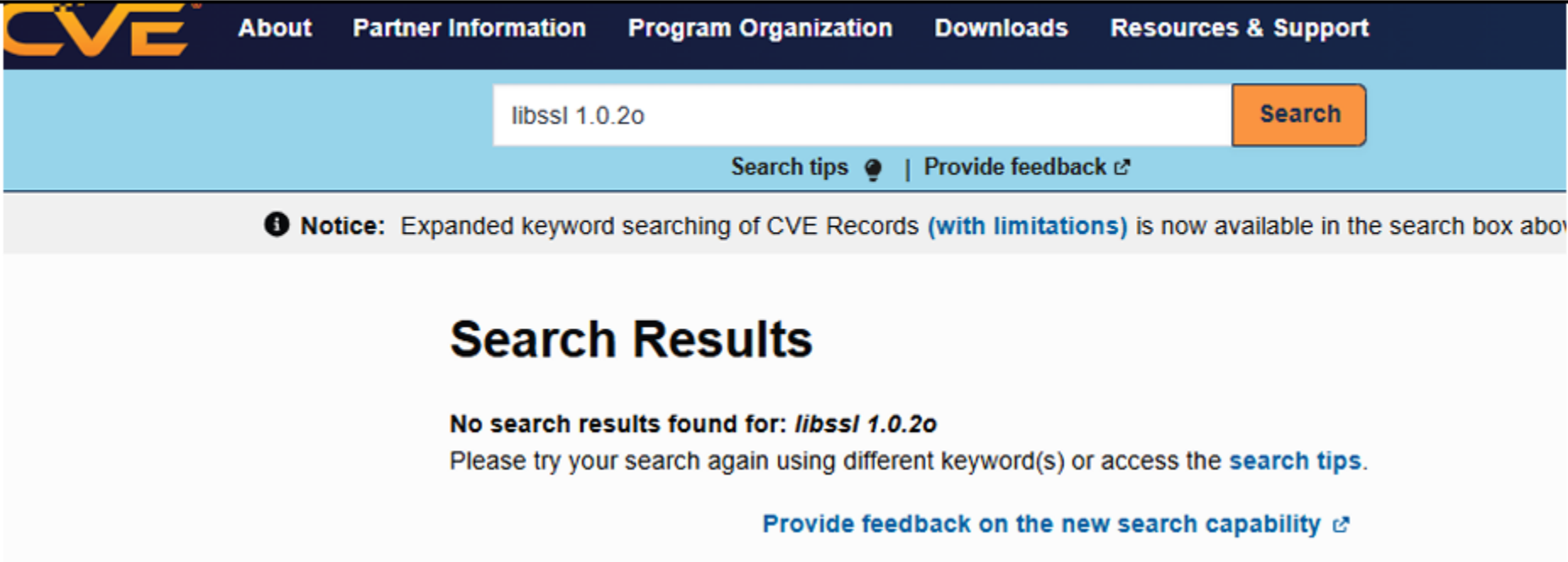
4.1.5.3.1. 檢測結果說明(1/3)

- 行動應用程式引用之第三方函式庫不存在已知 安全性漏洞，如本項檢測結果截圖說明之項次 1 至項次7 所示

項次	1		
圖示說明	15	引用函式庫名稱、版本、來源（包含作業系統內建及第三方函式庫）	<libssl / 1.0.2o / GPL> <libcrypto / 1.0.2o / GPL> <x264 / 1.4.2 / GPL> <libavcodec / 56.35.101 / LGPL> CoreTelephony AVFoundation MobileCoreService

4.1.5.3.1. 檢測結果說明(2/3)

- 行動應用程式引用之第三方函式庫不存在已知 安全性漏洞，如本項檢測結果截圖說明之項次 1 至項次7 所示

項次	3
圖示說明	 <p>The screenshot shows the CVE search interface. At the top, there is a navigation bar with links for 'About', 'Partner Information', 'Program Organization', 'Downloads', and 'Resources & Support'. Below this is a search bar containing the text 'libssl 1.0.20' and an orange 'Search' button. Under the search bar, there are links for 'Search tips' and 'Provide feedback'. A notice below the search bar states: 'Notice: Expanded keyword searching of CVE Records (with limitations) is now available in the search box above'. The main content area is titled 'Search Results' and displays the message: 'No search results found for: libssl 1.0.20. Please try your search again using different keyword(s) or access the search tips.' At the bottom of the search results area, there is a link: 'Provide feedback on the new search capability'.</p>

4.1.5.3.1. 檢測結果說明(3/3)

- 行動應用程式引用之第三方函式庫不存在已知 安全性漏洞，如本項檢測結果截圖說明之項次 1 至項次7 所示

項次	6
圖示說明	 <p>The screenshot shows the CVE search results page for the keyword "FFmpeg 2.6". The page displays a single result for CVE-2015-3395, which is a remote code execution vulnerability in the msrle_decode_pal4 function of the Libav library. The vulnerability affects versions of Libav before 10.7 and 11.x before 11.4, and FFmpeg before 2.0.7, 2.2.x before 2.2.15, 2.4.x before 2.4.8, 2.5.x before 2.5.6, and 2.6.x before 2.6.2. The page includes navigation controls such as "Previous", "Next", and "Back to top of page".</p> <p>註 : libavcodec 56.35.101 對應 FFmpeg 2.6.3</p>

4.1.5.4.1 檢測結果說明-不通過

- 檢查行動應用程式是否針對預期使用者輸入之字串驗證型別，如欄位本身需要接受特殊字元，亦屬於可預期的輸入字串型別。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。
- **不通過原因：無法證明是否有輸入特殊字元**



4.1.5.4.1 檢測結果說明-可供參考(1/2)

- 可證明對特殊字元之輸入有所限制或檢驗



4.1.5.4.1 檢測結果說明-可供參考(1/2)

(1). 檢查行動應用程式是否針對預期使用者輸入之字串驗證型別，如欄位本身需要接受特殊字元，亦屬於可預期的輸入字串型別。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。

電子信箱
!@#\$%^&* ()

密碼
.....|

登入

返回

忘記密碼

如果您還未註冊請點擊這裡進行註冊

查無帳號！
信箱格式錯誤

頁面	欄位	是否檢查/限制輸入
註冊帳號	身分證字號	是 (格式檢查)
	姓名	是 (無法輸入)
	電話號碼	是 (數字鍵盤)
	電子信箱	是 (格式檢查)
	密碼	為可預期的輸入字串型別
我的親友	姓名	是 (無法輸入)
	身分證字號	是 (格式檢查)
	電話號碼	是 (數字鍵盤)

4.1.5.4.1 檢測結果說明-可供參考(2/2)

(2). 檢查行動應用程式是否針對使用者輸入字串驗證長度。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。



頁面	欄位	是否檢查/字串長度
註冊帳號	身分證字號	是 (10)
	姓名	是 (2-50)
	電話號碼	是 (10)
	電子信箱	是 (255)
	密碼	是 (6-20)
我的親友	姓名	是 (2-50)
	身分證字號	是 (10)
	電話號碼	是 (10)

4.1.5.4.2 檢測結果說明-可供參考

- (1). 檢查行動應用程式是否防護使用者輸入 SQL Injection 字串之設計。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。



頁面	欄位	是否注入成功
註冊帳號	身分證字號	否
	姓名	否
	電話號碼	否
	電子信箱	否
	密碼	否
我的親友	姓名	否
	身分證字號	否
	電話號碼	否

感謝聆聽

也期待您的回饋，讓我們共創更有公信力的制度