

物聯網產品輔導介紹與案例 分享

財團法人台灣商品檢測驗證中心資通部

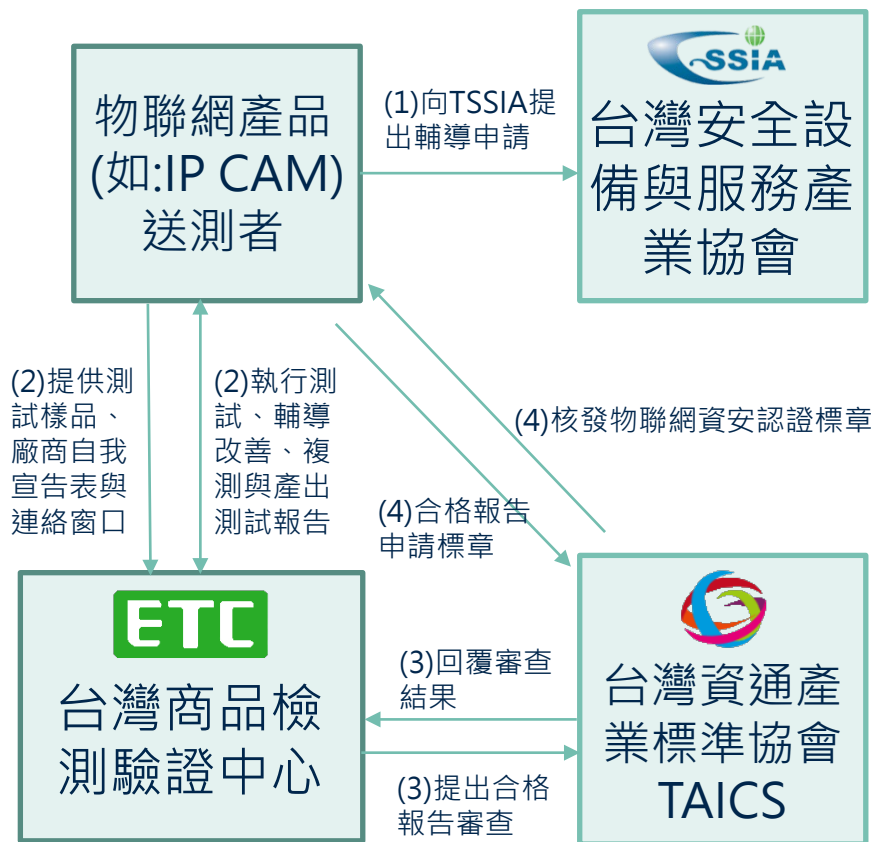
葉錫勳

2021年4月28日

簡 報 目 錄

- 一、物聯網產品資安輔導、測試與驗證流程
- 二、廠商自我宣告表填寫
- 三、案例分享

一、物聯網產品資安輔導、測試與驗證流程



(1) 向TSSIA提出測試申請

- 物聯網產品(如:IP CAM、NVR/DVR、NAS)業者向TSSIA提出受輔導標的申請。

(2) 執行測試、輔導改善、複測與產出測試報告

- 確認所有相關文件與送測標的均取得，開始測試
- 輔導改善：提供相關改善建議予廠商
- 複測：廠商經改善後再提供新版韌體進行複測。

(3) 向TAICS申請物聯網資安認證

- 交付相關文件：合格檢測報告。
- TAICS回覆審查結果。

(4) 取得物聯網資安認證標章

- 當合格報告經TAICS審查通過，則實驗室寄送合格報告給廠商。
- 廠商提出相關文件(含由TAICS審查通過的合格報告)向TAICS申請物聯網資安認證標章。
- TAICS核發物聯網資安認證標章給廠商。

二、廠商自我宣告表填寫(1/9)

填寫符合、不符合、部分符合或不支援等

針對該資安要求補充說明更詳細資訊，供實驗室判斷

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.1.1.1	產品預設不應透過實體介面存取產品作業系統之除錯模式。若需經實體介面存取，則應通過身分鑑別作業始得執行。	1級			產品若存在作業系統除錯介面，應於文件中說明進入作業系統除錯模式
5.1.1.2	卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。	2級(IP CAM)			

二、廠商自我宣告表填寫(2/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.1.2.1	產品應具有實體埠插拔操作記錄功能。	2級(IP CAM)			應提供產品之實體埠插拔紀錄的操作說明
5.1.2.2	產品應具備相關警示功能於實體操作發生斷訊時。	2級			應提供產品之異常警示機制功能說明
5.1.3.1	產品外部不應有徒手即可還原預設通行碼的功能。	1級			應提供產品之還原出廠設定操作說明。
5.1.4.1	產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。	3級			產品應提供安全啟動功能之設計文件。

二、廠商自我宣告表填寫(3/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.2.1	產品開啟之網路服務應為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商應於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。	1級			書面送審文件應包含產品啟用之網路服務與埠號的對應。
5.2.3.1	韌體應具備更新機制。	1級			(1) 應提供產品所使用之完整韌體。 (2) 應提供產品所使用之加密演算法書面資料作為審查依據。 (3) 若韌體經過加密處理，則廠商應提供解密工具。 (4) 應提供產品所有相連伺服器之宣告。

二、廠商自我宣告表填寫(4/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.3.2	產品若支援離線手動更新，則更新檔案應加密保護以確保機密性，且應採用 NIST SP 800-140C, CMVP Approved Security Functions(14)所核可之同等或以上加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或甚至可被解密回復之敏感性資料。	1級			(1) 應宣告更新伺服器之IP。 (2) 送測廠商應協助觸發產品韌體之線上更新。
5.2.3.4	產品應具備驗證韌體之完整性及真確性的功能。	1級			若選擇測試方法1 應提供產品之數位簽章使用機制。應提供產品所使用之韌體。

二、廠商自我宣告表填寫(5/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.3.5	產品應具備備援更新功能，即發生更新失敗時，系統能回復至更新前之狀態。	1級			其中斷時間點應是在韌體安裝(install)階段中斷更新，而非下載檔案期間。
5.2.4.1	產品所儲存的敏感性資料，應僅由獲授權個體存取。	1級			(1) 產品不存在作業系統的存取介面，則不適用此測項。 (2) 應提供產品所儲存之敏感性資料存取權限宣告作為審查依據。 (3) 若存在作業系統的存取介面，應提供能進入產品作業系統的方法。 (4) 應提供產品之系統管理者權限。

二、廠商自我宣告表填寫(6/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.4.2	產品所儲存之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)不應明文儲存，而保護資料的方式應採用NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。	1級			(1) 應提供產品所儲存之敏感性資料加密保護演算法作為審查依據。 (2) 應提供能進入產品作業系統的方法，及敏感性資料之存放位置。 (3) 應提供產品之系統管理者權限。 (4) 若產品具日誌功能，應提供檢視產品日誌之方法。 (5) 產品之根金鑰(root key)不適用此測項。

二、廠商自我宣告表填寫(7/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.4.3	產品應提出金鑰管理程序，以確保金鑰管理的品質。	2級			產品須提供金鑰管理程序之說明文件。
5.2.4.4	敏感性資料應存放於產品的安全區域(Security domain)，與正常作業環境隔離。	3級			(1) 應提供產品之敏感性資料儲存方式之書面資料作為審查依據。 (2) 應聲明產品具備哪些資安功能使用到安全區域之書面資料作為審查依據。
5.2.5.1	產品之網頁管理介面不應存在引發Injection 及Cross-Site Scripting (XSS)攻擊之漏洞。	1級			應提供產品網頁管理介面之系統管理者權限。

二、廠商自我宣告表填寫(8/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.6.1	ONVIF 應用程式介面，應具備身分鑑別機制，且其鑑別機制安全依5.4.1.1 及 5.4.1.2 之要求。	1級			(1) 產品未啟用ONVIF profile S，則不適用此測項。 (2) 應提供產品ONVIF 應用程式介面之角色存取權限之宣告。
5.2.6.2	ONVIF 應用程式介面，其通行碼鑑別安全依5.4.2 該要求項之所有要求。	1級			(1) 產品未啟用ONVIF profile S，則不適用此測項。 (2) 產品啟用ONVIF profile Q，則該測試項結果為不適用。但是應在產品之使用說明書或資安指引中註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件應公告在廠商官網上。 (3) 產品ONVIF 應用程式介面之使用者帳戶已建立。

二、廠商自我宣告表填寫(9/9)

測項	安全要求內容	安全等級	廠商自我宣告		備註
			是否符合	說明	
5.2.6.3(a)	ONVIF 應用程式介面，其權限管控依5.4.3 該要求項之所有要求。	1級			產品之ONVIF 應用程式介面未支援通行碼鑑別機制，則不適用此測項。
5.2.6.3(b)	ONVIF 應用程式介面，其權限管控依5.4.3 該要求項之所有要求。	1級			(1) 產品之ONVIF 應用程式介面未支援通行碼鑑別機制，則不適用此測項。 (2) 應提供產品ONVIF 應用程式介面之之帳戶鎖定機制之設計說明。

三、案例分享

測項：5.1.1.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.1.1實體埠之安全管控測試	5.1.1.1 實體介面安全管控測試	1級	查驗不能透過產品之實體介面或應透過身分鑑別，存取作業系統之除錯模式。	(1) 產品應保持出廠預設組態。 (2) 產品若存在作業系統除錯介面，應於文件中說明進入作業系統除錯模式之方法。

測試方法：

1. 檢視產品文件是否存在可進入作業系統除錯模式之實體介面。
2. 根據文件所述進入作業系統除錯模式之方法，開啟相應之管理介面連接工具。
3. 測試電腦連接產品之USB 埠。
4. 確認可否透過USB 埠存取作業系統之除錯模式。
5. 若存取前應經通行碼鑑別程序，則依照5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4測試通行碼鑑別機制之安全性。
6. 測試電腦連接產品之UART/JTAG 埠。
7. 確認可否透過UART/JTAG 埠存取作業系統之除錯模式。
8. 若存取前應經通行碼鑑別程序，則依照5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4測試通行碼鑑別機制之安全性。



新增測試JTAG埠

預期結果：

- 產品不存在進入作業系統除錯模式之介面。
- 產品透過USB、UART 及JTAG 存取作業系統之除錯模式時，產品要求通行碼鑑別，且符合5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4之測試結果。
- 通過：(1)(2)項結果符合其一。
- 不通過：(1)(2)項結果皆不符合。
- 不適用：無。

三、案例分享

範例：5.1.1.1 (2/2)

說明：若存在USB、UART、JTAG存取作業系統之除錯模式時，通行碼鑑別機制符合以下之測試預期結果。

5.4.2.1：是否有相同預設通行碼或首次上線後強制要求更改。

5.4.2.2：驗證通行碼長度。

5.4.2.3：驗證通行碼複雜度。

5.4.2.4：驗證通行碼的輸入頻率及次數限制。

可行作法：有些通過的廠商會將密碼管控機制做在web頁面。

三、案例分享

測項：5.1.2.2(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.1.2實體異常行為警示測試	5.1.2.2實體異常狀態警示機制	2級	查驗產品之網路服務遭受實體層阻絕時，有相應之警示機制。	無。

測試方法：

1. 若產品具有RJ-45 埠，透過RJ-45 埠連上網後，將網路線拔除，使主機因訊號中斷而無法連接上網路。
2. 檢視產品是否依照異常警示機制功能說明達到警示效果。
3. 若產品具有天線，透過天線連上網後，將天線遮罩，使主機因訊號中斷而無法連接上網路。
4. 檢視產品是否依照異常警示機制功能說明達到警示效果。

預期結果：

- 當產品具有RJ-45 埠，透過RJ-45 埠連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。
- 當產品具有天線，透過天線連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。
- 通過：(1)(2)項結果皆符合。
- 不通過：(1)(2)項結果不符合其一。
- 不適用：無。

三、案例分享

範例：5.1.2.2(2/2)

說明：

- 需主動發出警示，例如：聲音、彈跳視窗、推播通知、警示燈。
- 以實體手法中斷網路通訊時，產品**必須**主動發出警示，讓使用者知曉。

三、案例分享

測項：5.2.2.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.2網路服務連接埠管控測試	5.2.2.1網路服務最小化測試	1級	查證產品不能存在預期以外之網路埠。	書面送審文件應包含產品啟用之網路服務與埠號的對應。

測試方法：

1. 將測試電腦連接產品，啟用廠商所宣告之網路服務。
2. 啟動具網路埠掃描功能之工具，對產品執行TCP 與UDP 埠0 ~ 65535 之掃描。
3. 核對掃描結果所呈現之網路服務與對應埠。
4. 比對產品送審資料中所聲明之網路服務與對應埠。

預期結果：

- 通過：產品所開啟之網路服務與對應埠，與送審資料之內容相符
- 不通過：產品所開啟之網路服務與對應埠，與送審資料之內容不符。
- 不適用：無。

三、案例分享

範例：5.2.2.1(2/2)

說明：

1. 自我宣告須詳細記載所開啟的網路服務與對應埠。若有特殊情形：例如有開放卻未被掃出、隨機產生埠號等，應說明其功能與原因。
2. 自行檢測指令(使用nmap為例)：
nmap -p 0-65535 <ipcam ip>
nmap -sU -p 0-65535 <ipcam ip>

三、案例分享

測項：5.2.3.2(1/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.3更新安全測試	5.2.3.2韌體檔案安全測試	1級	查驗產品之韌體有經過加密保護。	(1) 產品不具備更新能力則不通過。 (2) 產品應支援離線更新，否則不適用此測試項。 (3) 應提供產品所使用之完整韌體。 (4) 應提供產品所使用之加密演算法書面資料作為審查依據。 (5) 若韌體經過加密處理，則廠商應提供解密工具。 (6) 應提供產品所有相連伺服器之宣告。 (7) 產品之根金鑰(root key)不適用此測項。

測試方法：

- (1) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。
- (2) 檢視該韌體更新檔是否可被解析出檔案系統目錄。
- (3) 若韌體更新檔無法被解析出檔案系統目錄，審閱可證明所使用加密演算法之書面資料。
- (4) 若韌體更新檔未加密，確認系統通行碼資料的保密機制是否採用NIST SP 800-140C, CMVP Approved Security Functions(2)所核可之安全功能。
- (5) 若韌體更新檔未加密，確認是否存在金鑰。
- (6) 若韌體更新檔未加密，確認是否存在非公開之email 資料。
- (7) 若韌體更新檔未加密，確認是否存在所宣告相連伺服器外之IP 資料。
- (8) 若韌體更新檔未加密，確認是否存在所宣告相連伺服器外之URL 資料。

預期結果(1/2)：

- 韌體具備更新功能。

三、案例分享

測項：5.2.3.2(2/3)

預期結果(2/2)：

- 韌體具備更新功能。
- 韌體更新檔案無法被解析出檔案系統目錄，且加密演算法採用NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。
- 韌體之程式碼與安裝檔內其他檔案，無檢出通行碼資料。
- 韌體之程式碼與安裝檔內其他檔案，無檢出加解密演算法之金鑰，或加解密金鑰不能被解密回復。
- 韌體之程式碼與安裝檔內其他檔案，不存在非公開email 資料。
- 韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之IP 資料。
- 韌體之程式碼與安裝檔內其他檔案，不存在所宣告相連伺服器外之URL 資料。
- 通過：(1)(2)項結果符合，或(1)(3)~(7)項結果皆符合。
- 不通過：不滿足(8)的測試結果。
- 不適用：產品具更新功能但不支援離線更新，或產品所儲存之根金鑰。



變更測試方法、測試結果：
實驗室提供測試金鑰，請廠商代為
簽章。

三、案例分享

測項：5.2.4.1 (1/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.4敏感性資料儲存安全測試	5.2.4.1敏感性資料權限管控測試	1級	查驗產品所儲存之敏感性資料於作業系統存取具有權限管控機制。	(1) 產品不存在作業系統的存取介面，則不適用此測項。 (2) 應提供產品所儲存之敏感性資料存取權限宣告作為審查依據。 (3) 若存在作業系統的存取介面，應提供能進入產品作業系統的方法。 (4) 應提供產品之系統管理者權限。

測試方法：

- (1) 將測試電腦連接產品。
- (2) 依據送測廠商所提供之進入作業系統方法，存取產品作業系統。
- (3) 檢視產品所儲存之通行碼存取權限。
- (4) 檢視產品所儲存之加解密金鑰存取權限。

預期結果：

- (1) 通過：產品通行碼及加解密金鑰之存取權限，與敏感性資料存取權限宣告相符。
- (2) 不通過：產品通行碼及加解密金鑰之存取權限，與敏感性資料存取權限宣告不符。
- (3) 不適用：產品不存在作業系統的存取介面。



如有進入作業系統之除錯方式，則由書面審查變為依廠商提供資料進行實際測試

三、案例分享

測項：5.2.4.2(1/4)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.4敏感性資料儲存安全測試	5.2.4.2敏感性資料加密儲存測試	1級	查驗產品之敏感性資料於儲存狀態下具有加密保護功能。	(1) 應提供產品所儲存之敏感性資料加密保護演算法作為審查依據。 (2) 應提供能進入產品作業系統的方法，及敏感性資料之存放位置。 (3) 應提供產品之系統管理者權限。 (4) 若產品具日誌功能，應提供檢視產品日誌之方法。 (5) 產品之根金鑰(root key)不適用此測項。

測試方法：

- (1) 審閱能證明符合此安全要求之書面資料。
- (2) 將測試電腦連接產品。
- (3) 依據送測廠商所提供之進入作業系統方法，及敏感性資料存放位置宣告，存取敏感性資料。
- (4) 檢視產品所儲存之通行碼及加解密用金鑰是否加密保護。
- (5) 若產品具日誌功能，檢視產品之日誌存在明文可識別之敏感性資料，例：密碼。

三、案例分享

測項：5.2.4.2(2/4)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.4敏感性資料儲存安全測試	5.2.4.2敏感性資料加密儲存測試	1級	查驗產品之敏感性資料於儲存狀態下具有加密保護功能。	(1) 應提供產品所儲存之敏感性資料加密保護演算法作為審查依據。 (2) 應提供能進入產品作業系統的方法，及敏感性資料之存放位置。 (3) 應提供產品之系統管理者權限。 (4) 若產品具日誌功能，應提供檢視產品日誌之方法。 (5) 產品之根金鑰(root key)不適用此測項。

預期結果：

(1) 通行碼及加解密金鑰採用NIST SP 800-140C, CMVP Approved Security

Functions 所核可之安全功能。

(2) 產品日誌不存在明文可識別之敏感性資料。

(3) 滿足5.2.4.4 的測試結果。

(4) 通過1：(1)(2)項皆符合。

(5) 通過2：(3)項符合

(6) 不通過：(1)(2)項任一不符合。

(7) 不適用：產品不會儲存通行碼及加解密金鑰，或產品所儲存之根金鑰。



1. 由書面審查變為依廠商提供資料進行實際測試
2. 測試結果要求變更通行碼及加解密金鑰採用NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。

三、案例分享

測項：5.2.5.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.5網頁管理介面安全測試	5.2.5.1網頁管理介面常見資安風險測試	1級	查驗產品之網頁管理介面不存在Injection 及XSS 資安風險漏洞。	應提供產品網頁管理介面之系統管理者權限。

測試方法：

- (1) 將測試電腦連接產品。
- (2) 開啟網頁管理介面。
- (3) 啟動具備網頁弱點掃描功能之工具，對產品網頁介面執行弱點掃描。
- (4) 檢視該弱點掃描工具所產生之報告，是否存在引發Injection 及Cross-Site Scripting (XSS)之資安攻擊風險。

預期結果：

- 通過：產品之網頁管理介面，不存在引發Injection 及XSS 資安攻擊風險。
- 不通過：產品之網頁管理介面，存在引發Injection 及XSS 資安攻擊風險。
- 不適用：產品無網頁管理介面。

三、案例分享

範例：5.2.5.1(2/2)

常見問題與改善方式：

1.關於X-XSS-Protection，需要於WebServer加入Header設定

X-XSS-Protection:1; mode=block。

2.關於X-Content-Type-Options，需於WebServer加入Header設定

X-Content-Type-Options:nosniff

三、案例分享

測項：5.2.6.2(1/5)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.6 ONVIF (Open Network Video Interface Forum)應用程式介面(API)安全測試	5.2.6.1 ONVIF 應用程式介面之鑑別機制測試	1級	查驗產品之ONVIF 應用程式介面呼叫應經過鑑別程序，且該鑑別程序具備重送攻擊抵抗能力，並鑑別錯誤訊息未揭露敏感性資料。	(1) 產品未啟用ONVIF profile S，則不適用此測項。 (2) 產品啟用ONVIF profile Q，則該測試項結果為不適用。但是應在產品之使用說明書或資安指引中註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件應公告在廠商官網上。 (3) 產品ONVIF 應用程式介面之使用者帳戶已建立。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 開啟電腦或行動裝置之ONVIF 操控程式。
- (3) 執行影像監控相關操作，並執行封包側錄。
- (4) 輸入已存在之使用者帳戶搭配錯誤的通行碼，檢視鑑別錯誤訊息。
- (5) 輸入不存在之使用者帳戶，檢視鑑別錯誤訊息。
- (6) 透過操控程式與產品建立連線，同時側錄封包。
- (7) 執行影像監控相關操作，檢視封包側錄結果是否要求身分鑑別。
- (8) 若產品要求身分鑑別，將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至受測產品。
- (9) 檢視鑑別結果是否成功。
- (10) 若產品啟用ONVIF profile Q，則審閱使用說明或資安指引之相關聲明。

三、案例分享

測項：5.2.6.2(2/5)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.6 ONVIF (Open Network Video Interface Forum)應用程式介面(API)安全測試	5.2.6.1 ONVIF 應用程式介面之鑑別機制測試	1級	查驗產品之ONVIF 應用程式介面呼叫應經過鑑別程序，且該鑑別程序具備重送攻擊抵抗能力，並鑑別錯誤訊息未揭露敏感性資料。	(1) 產品未啟用ONVIF profile S，則不適用此測項。 (2) 產品啟用ONVIF profile Q，則該測試項結果為不適用。但是應在產品之使用說明書或資安指引中註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件應公告在廠商官網上。 (3) 產品ONVIF 應用程式介面之使用者帳戶已建立。

預期結果：

- (1) 透過ONVIF 應用程式介面存取產品時有要求身分鑑別，且重送攻擊對該身分鑑別無效。
- (2) 該身分鑑別錯誤訊息無法推斷出合法使用者帳戶或通行碼。
- (3) 產品啟用ONVIF profile Q，產品之使用說明書或資安指引有註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件公告在廠商官網上。
- (4) 通過：(1)(2)項結果符合，或(3)項結果符合。
- (5) 不通過：不滿足(4)的測試結果。
- (6) 不適用：產品未啟用ONVIF profile S。

三、案例分享

測項：5.2.7.1(1/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.7日誌檔與警示測試	5.2.7.1安全事件日誌檔測試	1級	查驗產品有安全事件日誌供查詢。	(1) 應提供安全事件日誌之查詢方法。 (2) 若產品之安全事件日誌由後台伺服器記錄，則應提供可對接之後台伺服器進行測試。 (3) 若產品之安全事件日誌由後台伺服器記錄，則應提供使用說明或資安指引供審。

測試方法：

1. 將測試電腦或行動裝置連接產品。
2. 依產品使用說明，開啟相對應之管理介面連接工具，瀏覽安全事件日誌。
3. 檢視日誌內容是否記載使用者的登入紀錄，包括時間(含年、月、日、時、分、秒)、登入後之使用者身分及登入成功與否。
4. 將產品重新開機。
5. 檢視重開機前之安全事件日誌資料是否存在。
6. 若產品之安全事件日誌皆記錄於後台伺服器中則側錄送往後台之安全事件日誌封包。
7. 審閱使用說明或資安指引之相關安全日誌聲明。

三、案例分享

測項：5.2.7.1(2/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.7日誌檔與警示測試	5.2.7.1安全事件日誌檔測試	1級	查驗產品有安全事件日誌供查詢。	(1) 應提供安全事件日誌之查詢方法。 (2) 若產品之安全事件日誌由後台伺服器記錄，則應提供可對接之後台伺服器進行測試。 (3) 若產品之安全事件日誌由後台伺服器記錄，則應提供使用說明或資安指引供審。

預期結果：

1. 產品具有可供使用者檢視之安全事件日誌功能。
2. 產品之安全事件日誌資料，包含時間、登入後之使用者身分及登入成功與否。
3. 重開機前之安全事件日誌仍可查詢。
4. 若產品之安全事件日誌由後台伺服器記錄，則產品送往後台之安全事件日誌封包的資料，至少包含時間、登入後之使用者身分及登入成功與否。
5. 若產品之安全事件日誌由後台伺服器記錄，則應於使用說明書或資安指引中聲明此情境，且該文件公告在廠商官網上。
6. 通過：(1)~(3)項結果符合，或(4)(5)項結果皆符合。
7. 不通過：不滿足(6)的測試結果。
8. 不適用：無。



前置條件、測試結果變更：
 增加：若產品提供有後台伺服器之安全事件日誌記錄，則應提供可對接之後台伺服器進行測試，且應提供使用說明或資安指引供審。

三、案例分享

範例：5.2.7.1(3/3)

登入資訊

於此區您可以檢視所有系統狀態

啟動時間記錄

於此區您可以檢視系統最後重新啟動時間

2018-09-07 12:46:05

除錯訊息

於此區域將顯示除錯訊息

```
----- beginning of main
09-07 04:49:09.540 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
CPU5: device=cluster1 frequency=1804800
09-07 04:49:09.591 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=998400
09-07 04:49:09.642 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=1056000
09-07 04:49:09.693 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=1113600
09-07 04:49:09.919 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=940800
09-07 04:49:09.919 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
CPU5: device=cluster1 frequency=1804800
09-07 04:49:10.022 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
CPU5: device=cluster1 frequency=1804800
09-07 04:49:10.125 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=883200
09-07 04:49:10.125 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
CPU5: device=cluster1 frequency=1804800
09-07 04:49:10.176 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=940800
09-07 04:49:10.227 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
L2_CACHE_1: device=cluster1 frequency=998400
09-07 04:49:10.227 451 653 | ThermalEngine: cpu_frequency_pre_req: SS-
```

系統日誌

於此區顯示系統日誌

```
[33579009/12000000/0]!!!!
<6>[ 97.206904] MSM_GFP msm_cpp_subdev_ioctl:2794 stream_cnt:0
<6>[ 97.303160] rtc-ds3232 2-0068: [AVC][RTC], read_time 2018/09/07 04:47:42
<6>[ 97.304546] rtc-ds3232 2-0068: [AVC][RTC], read_time 2018/09/07 04:47:42
<3>[ 97.416010] msm_isp_notify: PIX0 frame id: 1
```

說明：安全事件日誌的資料包含正確時間(包括年、月、日、時、分、秒)，但未提供使用者身分及執行結果。

三、案例分享

測項：5.2.7.3(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.2.7日誌檔與警示測試	5.2.7.3安全事件日誌檔之日誌滾動功能測試	1級	查驗產品具處理日誌儲存空間不足之異常狀況的能力。	(1) 產品之安全事件日誌皆記錄於後台伺服器中，則不適用此測項。 (2) 應提供產品之系統管理者權限。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 不斷觸發安全事件日誌，以填充安全事件紀錄儲存空間，直到發生日誌儲存空間循環使用。
- (3) 檢視產品是否無法正常記錄安全事件。

預期結果：

- (1) 通過：產品仍可正常記錄安全事件。
- (2) 不通過：產品發生儲存空間不足的現象。
- (3) 不適用：產品之安全事件日誌皆記錄於後台伺服器中。



前置條件、測試結果新增：不適用：產品之安全事件日誌皆記錄於後台伺服器中。

三、案例分享

範例：5.2.7.3(2/2)

說明：

須提供安全日誌滾動機制的設計說明。(例如：儲存容量、日誌滾動機制等)

三、案例分享

測項：5.3.1.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.3.1資料傳輸安全測試	5.3.1.1敏感性資料之傳輸保護初階測試	1級	查驗產品敏感性資料之傳輸，預設採用強度足夠之安全通道。	產品應保持出廠預設組態。

測試方法：

1. 掃描產品使用之安全通道。
2. 比對掃描結果是否為附錄A中所包含之密碼套件。
3. 將測試電腦及行動裝置連接產品。
4. 登入相對應之管理介面，同時側錄封包。
5. 檢視所側錄之封包是否採用安全通道傳輸。

預期結果：

- (1) 安全通道僅採用附錄A中所建議之密碼套件。
- (2) 與測試電腦之間的帳戶通行碼資訊傳輸，預設採用安全通道。
- (3) 與行動裝置之間的帳戶通行碼資訊傳輸，預設採用安全通道。
- (4) 通過：(1)~(3)項結果皆符合。
- (5) 不通過：(1)~(3)項結果不符合其一。
- (6) 不適用：產品不存在敏感性資料。



1.不進行憑證置換測試
2.新增不適用：產品不存在敏感性資料。

三、案例分享

範例：5.3.1.1(2/2)

Starting Nmap 7.70 (<https://nmap.org>) at 2019-02-15 11:54 ㄗxㄗ_?D·CRE?!
Nmap scan report for 192.168.0.42
Host is up (0.0010s latency).

```
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http thttpd 2.25b (PHP 20030920)
|_http-server-header: thttpd/2.25b PHP/20030920
ssl-enum-ciphers:
  TLSv1.0:
    ciphers:
      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 2048) - A
      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
      TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
      TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A
    compressors:
      NULL
    cipher preference: client
    warnings:
      64-bit block cipher 3DES vulnerable to SWEET32 attack
      64-bit block cipher IDEA vulnerable to SWEET32 attack
      Broken cipher RC4 is deprecated by RFC 7465
      Ciphersuite uses MD5 for message integrity
  TLSv1.1:
    ciphers:
      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
      TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
      TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 2048) - A
      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
      TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
      TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
      TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
      TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A
    compressors:
```

不符合之案例

附錄 A
(規定)

符合之案例

安全通道應使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
 - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_CCM_SHA256
 - TLS_AES_128_CCM_8_SHA256

三、案例分享

測項：5.4.2.4(1/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.4.2通行碼鑑別安全測試	5.4.2.4通行碼的輸入頻率及次數限制	1級	查驗產品之通行碼鑑別機制具防止暴力破解之能力。	(1) 產品未支援通行碼鑑別機制，則不適用此測項。 (2) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立。 (3) 應提供產品之帳戶鎖定機制之設計說明。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 根據產品使用說明，開啟相對應之管理介面連接工具以執行鑑別。
- (3) 不斷輸入錯誤且相異的通行碼。
- (4) 檢視產品於帳戶或IP 鎖住計數器重設為0 前，廠商宣告計數器重設時限內連續登入不成功次數5 次以內，會鎖住帳戶或IP。
- (5) 鎖住帳戶或IP 後，於鎖住期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳戶或IP 鎖住時限內，檢視帳戶或IP 是否解鎖。
- (6) 同一帳戶或IP 任一次登入不成功後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入不成功次數是否重新計算。
- (7) 若產品採用的密碼強度原則是國際標準要求或公認之資安產業慣例之規格，檢視其來源與安全強度是否足夠信任。

三、案例分享

測項：5.4.2.4 (2/3)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.4.2通行碼鑑別安全測試	5.4.2.4通行碼的輸入頻率及次數限制	1級	查驗產品之通行碼鑑別機制具防止暴力破解之能力。	(1) 產品未支援通行碼鑑別機制，則不適用此測項。 (2) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立。 (3) 應提供產品之帳戶鎖定機制之設計說明。

預期結果：

- (1) 輸入次數5次以內，會鎖住帳戶或IP。
- (2) 於廠商宣告之帳戶或IP鎖住時限內，帳戶或IP未解鎖。
- (3) 於廠商宣告計數器重設時限內，不成功次數未重新計算。
- (4) 產品採用鎖住IP來防止暴力破解，則產品同時應具備可限制被連結IP之功能。
- (5) 採用之密碼強度原則出自國際標準或符合公認資安產業慣例。
- (6) 通過：(1)~(4)項皆符合，或(5)項符合。
- (7) 不通過：不滿足(6)的測試結果。
- (8) 不適用：產品未支援通行碼鑑別機制。



1.新增鎖住IP
2.採用之密碼強度原則出自國際標準或符合公認資安產業慣例。

三、案例分享

範例：5.4.2.4(3/3)

說明：

很多廠商在web介面都沒有做該機制。

此外，如有支援ONVIF或USB、UART介面登入作業系統功能，亦須符合本測項要求。

三、案例分享

測項：5.4.3.2(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.4.3權限管控測試	5.4.3.2權限有效時間	1級	查驗產品存在有限的授權期限。	(1) 產品之使用者帳戶及相關鑑別因子(例：通行碼)已建立。 (2) 產品之使用情境必須為常時間使用不間斷(例：大樓監視器)，則廠商應於文件中聲明，並在使用指南或安全指引中註明建議補償做法。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 檢視產品之網頁管理介面，存在供使用者設定的閒置時限操作介面。
- (3) 閒置產品直到超過閒置時限值。
- (4) 檢視需重新鑑別方可存取產品。

預期結果：

- (1) 產品之授權行為，存在閒置時限供使用者設定。
- (2) 遠端連線閒置逾時，應經過鑑別方可存取產品。
- (3) 產品之使用情境必須為常時間使用不間斷，則廠商於產品使用指南或安全指引中，聲明建議安全的補償做法。
- (4) 通過1：(1)(2)項結果皆符合。
- (5) 通過2：(3)項結果符合。
- (6) 不通過：「通過1」及「通過2」皆不符合。
- (7) 不適用：無。

新增測試結果：產品之使用情境必須為常時間使用不間斷，則廠商於產品使用指南或安全指引中，聲明建議安全的補償做法。

三、案例分享

範例：5.4.3.2(2/2)

說明：

多數受測標的未檢出有提供閒置時限操作介面(測試規範：產品之授權行為，存在閒置時限供使用者設定。)

三、案例分享

測項：5.5.1.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.5.1隱私資料的存取保護測試	5.5.1.1隱私資料的存取控制	1級	驗證產品隱私權是否具有存取控制機制。	(1) 產品須提供隱私存取權限之宣告。 (2) 產品必須能建立 2 個以上的帳號，否則此測項不適用。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 從網頁管理介面，分別以不同角色登入產品。
- (3) 存取影像資料，同時檢視該帳戶之角色與其對應之隱私存取權限與廠商宣告相符。
- (4) 當產品提供網頁管理介面且已經有帳戶登入的情況下，檢視無需透過帳戶切換，即可存取該帳戶權限之外的隱私資料。

預期結果：

- (1) 通過：使用者的隱私存取授權與廠商宣告相符。
- (2) 不通過：使用者的隱私存取授權與廠商宣告不符。
- (3) 不適用：無。

三、案例分享

範例：5.5.1.1(2/2)

說明：

範例1：由不同角色登入時，若隱私資料存於SD卡，則該角色**只能存取自行錄製的隱私資料**。(以前的作法)

範例2：僅有管理者權限可存取SD卡上的隱私資料，其餘角色皆無存取權限。

三、案例分享

測項：5.5.1.2(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.5.1隱私資料的存取保護測試	5.5.1.2 隱私外洩警示功能測試	1級	查驗產品具有防止隱私外洩之功能。	(1) 應提供產品之隱私外洩警示功能說明。 (2) 若登入警示應搭配後台伺服器運行，則應提供可對接之後台伺服器進行測試。 (3) 若登入警示應搭配後台伺服器運行，則應提供使用說明或資安指引供審。

測試方法：

- (1) 將測試電腦或行動裝置連接產品。
- (2) 透過網頁管理介面或操控程式，以不同角色登入產品。
- (3) 存取影像資料。
- (4) 確認系統管理者或已登入使用者是否接收到警示。
- (5) 若產品之登入警示由後台伺服器執行，則側錄送往後台之登入警示相關之封包。
- (6) 若產品之登入警示由後台伺服器執行，則審閱使用說明或資安指引之相關登入警示聲明。

預期結果：

- (1) 每次發生新的使用者登入或登入以存取影像事件時，產品發出警示。
- (2) 若產品之登入警示由後台伺服器執行，則應於使用說明書或資安指引中聲明此情境，且該文件公告在廠商官網上
- (3) 通過：(1)(2)項任一符合。
- (4) 不通過：(1)(2)項皆不符合。
- (5) 不適用：無。

三、案例分享

範例：5.5.1.2(2/2)

說明：

範例1：當發生新的產品存取事件時(登入成功或失敗)，產品發出email通知。

範例2：當發生新的產品存取事件時(登入成功或失敗)，web介面跳出視窗通知。

三、案例分享

測項：5.5.2.1(1/2)

安全要求分項	測試項目	安全等級	測試目的	樣品條件
5.5.2隱私資料的傳輸保護測試	5.5.2.1隱私資料之傳輸保護初階測試	1級	查驗產品影像資料之傳輸，預設採用強度足夠之安全通道。	產品應保持出廠預設組態。

測試方法：

- (1) 掃描產品使用之安全通道。
- (2) 比對掃描結果是否為附錄A 中所包含之密碼套件。
- (3) 將測試電腦及行動裝置連接產品。
- (4) 於相應之管理介面啟動影像監控功能，同時側錄封包。
- (5) 檢視所側錄之封包是否採用安全通道傳輸。

預期結果：

- (1) 安全通道僅採用附錄A 中所建議之密碼套件。
- (2) 與測試電腦之間的影像資料傳輸，預設採用安全通道。
- (3) 通過：(1)(2)項結果皆符合。
- (4) 不通過：(1)(2)項結果不符合其一。
- (5) 不適用：無。

三、案例分享

範例：5.5.2.1(2/2)

說明：

安全通道須僅支援「附錄 A」中所建議之密碼套件。

附錄 A

(規定)

安全通道應使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
 - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_CCM_SHA256
 - TLS_AES_128_CCM_8_SHA256

簡報結束 敬請指教

資訊與通信技術服務部

葉錫勳

E-mail : eacn@etc.org.tw

電話：03-3280026轉621

王煜詔

E-mail : taichi@etc.org.tw

電話：03-3280026轉562



附錄、改版差異(1/13)

新版	舊版
5.1.1.1 1. 新增測試JTAG埠	5.1.1.1
5.1.2.1 1. 測試結果修改： 插拔操作紀錄包含正確時間格式(包括年、月、日、時、分、秒)、使用者身分及執行結果。	5.1.2.1 1.該實體埠插拔記錄之時間正確。
5.1.2.2 1. 測試結果修改： (1) 當產品具有RJ-45 埠，透過RJ-45埠連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。 (2) 當產品具有天線，透過天線連線後發生斷訊狀況時，產品發出警示(例：電子郵件、推播、閃光、音效等)。	5.1.2.2 1.發生斷訊狀況時，產品發出警示。

附錄、改版差異(2/13)

新版	舊版
5.2.1.1 (a) 測試作業系統是否存在CVSS v3.0 評分為9.0 分以上之常見資安弱點與漏洞初階測試	5.2.1.1 測試作業系統是否存在CVSS v3 評分為9.0 分以上之常見資安弱點與漏洞
5.2.1.1 (b) 測試作業系統是否存在CVSS v3.0 評分為9.0 分以上之常見資安弱點與漏洞中階測試	
5.2.2.2遙測資料收集測試：新增測項 - 將產品連接網際網路，使用封包側錄工具，將受測物於連網狀態下持續側錄至少24 小時。 - 檢視側錄結果是否存在產品所宣告之相連伺服器外之IP 及/或URL 資料。	無此測項

附錄、改版差異(3/13)

新版	舊版
5.2.3.1 韌體更新功能測試: 新增測項 (b)測試目的： 查驗產品具韌體更新功能。	
5.2.3.2韌體檔案安全測試 產品之根金鑰(root key)不適用此測項 (b) 查驗產品之韌體有經過加密保護。 單一情境測試	5.2.3.1 (a)韌體檔案安全測試 (b)測試目的： 驗證產品之韌體更新檔是否會洩露敏感性資料。 分成兩情境測試
5.2.3.3韌體更新路徑的保護 測試結果新增： (1) 韌體具備更新功能。	5.2.3.1 (b)韌體更新路徑的保護

附錄、改版差異(4/13)

新版	舊版
5.2.3.4 韌體更新檔之完整性及真確性測試 變更測試方法、測試結果： 實驗室提供測試金鑰，請廠商代為簽章。	5.2.3.2 韌體更新檔之完整性及可信度測試
5.2.3.5 備援更新功能測試 變更為單一情境測試	5.2.3.3 備援更新功能測試 有兩測試情境：離線手動、線上更新
5.2.4.1 敏感性資料權限管控測試 如有進入作業系統之除錯方式，則由書面 審查變為依廠商提供資料進行實際測試	5.2.4.1 敏感性資料權限管控測試 分為初階(1級)書審、中階測試(2級)實測
5.2.4.2 敏感性資料加密儲存測試 1. 由書面審查變為依廠商提供資料進行實際測試 2. 測試結果要求變更 通行碼及加解密金鑰採用NIST SP 800-140C, CMVP Approved Security Functions 所核可之安全功能。	5.2.4.2 敏感性資料加密儲存測試 1. 分為初階(1級)書審、中階測試(2級)實測 2. 測試結果要求 加密演算法的選用需依循FIPS 140-2

附錄、改版差異(5/13)

新版

~~5.2.6.1~~ **5.2.6.3** ONVIF 應用程式介面之權限管控機制測試
適用條件變更：產品未啟用 ONVIF profile S，則不適用此測項。

~~5.2.6.2~~ **5.2.6.1** ONVIF 應用程式介面之鑑別機制測試
前置條件變更：

1. 產品未啟用 ONVIF profile S，則不適用此測項。
2. 用 ONVIF profile Q，則該測試項結果為不適用。但是應在產品之使用說明書或資安指引中註明：「產品於出廠預設組態(factory default state)下，不建議連接網際網路。」，且該文件應公告在廠商官網上。

舊版

5.2.6.3 應用程式介面之權限管控機制

5.2.6.1 應用程式介面之鑑別機制測試
(a)應用程式介面之鑑別機制強度測試
側錄封包後重送攻擊，該身分鑑別程序具備重送攻擊抵抗能力。
(b)應用程式介面之身分鑑別錯誤訊息
驗證鑑別錯誤訊息不會造成敏感性資料的洩漏。

附錄、改版差異(6/13)

新版

~~5.2.6.3 (a) ONVIF 應用程式介面之通行碼鑑別強度提示測試~~

~~(b) 測試目的：~~

~~查驗產品之ONVIF 應用程式介面之通行碼鑑別機制強度不足時應提示。~~

~~測試結果變更：~~

~~通行碼鑑別機制符合5.4.2.1 之測試結果~~

~~5.2.6.3 (b) 5.2.6.2~~ ONVIF 應用程式介面之通行碼鑑別強度機制測試

(b) 測試目的：

查驗產品之ONVIF 應用程式介面的通行碼鑑別機制強度應足夠。

測試步驟、結果變更：

需側錄封包，且結果符合通行碼鑑別機制符合5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4之測試預期結果。

舊版

5.2.6.2 應用程式介面之通行碼鑑別強度機制測試

測試結果：

通行碼鑑別機制符合 5.4.2.1、5.4.2.2、5.4.2.3、5.4.2.4 之測試預期結果。

附錄、改版差異(7/13)

新版	舊版
<p>5.2.7.1 安全事件日誌測試 前置條件、測試結果變更： 增加：若產品提供有後台伺服器之安全事件日誌記錄，則應提供可對接之後台伺服器進行測試，且應提供使用說明或資安指引供審。</p>	<p>5.2.7.1 安全事件日誌檔測試 僅考慮本機安全事件日誌之可用性</p>
<p>5.2.7.2 安全事件日誌檔存取權限管控測試 測試結果新增：不適用：產品之安全事件日誌皆記錄於後台伺服器中。</p>	<p>5.2.7.2 安全事件日誌檔存取權限管控測試 僅考慮本機安全事件日誌之可用性</p>
<p>5.2.7.3 安全事件日誌檔之日誌滾動功能測試 前置條件、測試結果新增：不適用：產品之安全事件日誌皆記錄於後台伺服器中。</p>	<p>5.2.7.3 安全事件日誌檔之日誌滾動功能測試 僅考慮本機安全事件日誌之可用性</p>

附錄、改版差異(8/13)

新版	舊版
無此測項	5.2.7.4異常警示功能測試
5.3.1.1 敏感性資料之傳輸保護初階測試 測試： 1. 不進行憑證置換測試 2. 新增不適用：產品不存在敏感性資料	5.3.1.1 敏感性資料之傳輸保護初階測試 測試： 有憑證置換測試
5.3.1.2 敏感性資料之傳輸保護中階測試 測試結果變更： 1. 進行憑證置換測試 2. 新增不適用：產品不存在敏感性資料	5.3.1.2 敏感性資料之傳輸保護中階測試
5.3.1.3 敏感性資料之傳輸保護高階測試 測試結果： 新增：不適用：產品不具備安全通道功能	5.3.1.2 敏感性資料之傳輸保護中階測試 測試結果： 該安全通道支援AES-256 同等或以上加密強度的演算法。

附錄、改版差異(9/13)

新版	舊版
5.4.1.1 測試方法變更： 當產品具網頁管理介面，嘗試在未登入情況下，存取錄影監控頁面。 測試結果變更： (1) 產品具備身分鑑別機制且身分鑑別功能 不能被關閉 ，同時鑑別機制具備抵抗重送攻擊的能力。	5.4.1.1 網頁介面鑑別安全測試
5.4.1.2 身分鑑別錯誤訊息測試 測試結果： 新增：不適用：產品不支援身分鑑別機制	5.4.1.2 身分鑑別錯誤訊息
5.4.1.3 憑證更換功能測試 前置條件、測試結果新增： 產品不存在憑證鑑別之功能，則此測項不適用。	5.4.1.3 憑證上傳介面測試

附錄、改版差異(10/13)

新版	舊版
5.4.1.4 金鑰唯一性測試 前置條件新增：產品之根金鑰(root key) 不適用此測項。	5.4.1.4 金鑰唯一性測試
5.4.2.1 預設通行碼安全 整併測試情境 (b) 測試目的： 查驗產品沒有相同的預設通行碼或預設通行碼會於首次上線後強制要求更改。	5.4.2.1 預設通行碼安全 分成兩測試情境 (b)測試目的： (1) 情境1： 驗證產品是否有相同的預設通行碼。 (2) 情境2： 驗證產品預設通行碼是否會於首次上線後強制要求更改。
5.4.1.4 金鑰唯一性測試 前置條件新增：產品之根金鑰(root key) 不適用此測項。	5.4.1.4 金鑰唯一性測試
5.4.2.2 通行碼長度 新增測試結果：採用之密碼強度原則出自國際標準或符合公認資安產業慣例。	5.4.2.2 通行碼長度

附錄、改版差異(11/13)

新版	舊版
5.4.2.3 通行碼複雜度 新增測試結果：採用之密碼強度原則出自國際標準或符合公認資安產業慣例。	5.4.2.3 通行碼複雜度
5.4.2.4 通行碼的輸入頻率及次數限制 測試結果修改： 1. 新增鎖住IP 2. 採用之密碼強度原則出自國際標準或符合公認資安產業慣例。	5.4.2.4 通行碼的輸入頻率及次數限制
5.4.2.5 通行碼連續字元之避免 新增測試結果： 採用之密碼強度原則出自國際標準或符合公認資安產業慣例。	5.4.2.5 通行碼連續字元之避免
5.4.2.6 通行碼歷程記錄 新增測試結果： 採用之密碼強度原則出自國際標準或符合公認資安產業慣例。	5.4.2.6 通行碼歷程記錄

附錄、改版差異(12/13)

新版	舊版
5.4.3.1 權限管控機制 新增測試結果：至少有2 個以上不同權限的角色，若此功能會對營運產生不利影響產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。	5.4.3.1 權限管控機制
5.4.3.2 權限有效時間 新增測試結果：產品之使用情境必須為常時間使用不間斷，則廠商於產品使用指南或安全指引中，聲明建議安全的補償做法	5.4.3.2 權限有效時間
5.5.1.2 隱私外洩警示功能測試 新增測項	

附錄、改版差異(13/13)

新版	舊版
無此測項	5.5.1.2 隱私資料刪除功能
無此測項	5.5.1.3 登入警示功能測試
5.5.2.2 隱私資料之傳輸保護中階測試 預期結果： 已竄改影像資料傳輸用之安全通道憑證未通過產品鑑別。	
5.1.1.2 最小實體介面測試 測試目的： 查驗是否可徒手從產品外部取得儲存媒體	5.1.1.2 最小實體介面測試 測試目的： 查驗是否可輕易從產品外部取得儲存媒體
5.1.3.2 實體保護測試 前置條件、測試結果新增： 若產品之外殼拆除障礙，是透過現場佈建時，額外於產品外殼再裝上支架或防護罩外殼來加以保護，廠商應在產品之使用的類型，且該文件應公告在廠商官網上。	5.1.3.2 實體保護測試