IP_CAM改版

高傳凱 博士

前次會議決議事項

1. 資策會將於下次會議提出合適的滲透測試執行方法，並提供現場專家討論以制定出合適的執行方法。

2. ISO 27001因為是管理安全，跟產品安全無關，現場專家一致反對駁回，不再討論。

3. 下次會議將會再討論晶片安全應要滿足的安全要求。

本次討論主題

- 新增測試手法執行細節討論: 滲透測試
- 前次會期增修之測試實驗室項目
- 隱私/國安資料洩漏測試
- 臨時動議: 晶片資安

議案1: 多元化資安檢測方法導入

- 實驗室所採用的資安檢測方法，其能**支持與證明一致性的達到本標準的要求**，並確保檢測結果品質，實驗室應依據選項A或選項B，實施資安檢測
  - 選項A: 採用TAICS TS 0015 series測試規範中的測試方法執行。
  - 選項B: 採用滲透測試方法執行。
- 實施對策:
  - 為確保此方案實施後能確實滿足標準需求，依流程必須先執行**檢測試行**。
  - 請**提案單位**論證滲透測試的可執行性，論證結果(測試報告)可視情況作為未來產品驗證審查之依據。

議案2: 5.2.4.4敏感性資料隔離保護

- 問題
  - 與5.2.4.2是一樣的測試目的，但是2項的測試方法是互斥的，且5.2.4.4強度更強
- 解決方法
  - 5.2.4.2的通過條件裡會增加:「滿足5.2.4.4通過條件，即會通過5.2.4.2」

通過條件:

(i)產品滿足 5.2.4.4 通過條件，則此測試結果為通過。↵

~~(i)~~(ii)通行碼資料的保密機制採用 FIPS 140-2 Annex A 所核可之單向雜湊函數(one-way hash)。↵

~~(ii)~~(iii)敏感性資料(含加解密用金鑰)的保密機制採用 FIPS 140-2 Annex A 所核可之加密演算法。↵

議案3: 5.2.6.2/5.4.2 密碼強度

- 因應實際應用情境且有更佳的密碼強度實務原則，條文建議修改如下:

測試步驟

步驟 1： 將測試電腦或行動裝置連接產品。
步驟 2： 從網頁管理介面或操控程式建立或變更通行碼。
步驟 3： 輸入小於 8 個字元長度之通行碼，檢查是否發出警示。
步驟 4： 輸入僅同時含下述四者字元中的一種及二種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.10 進位數字 (0 到 9)；4.非英文字母字元 (例如： !、$、#、%)，檢查通行碼是否能成功建立或變更，檢查是否發出警示。
步驟 5： 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

提議2、3級不適用

通過條件

(1) 執行步驟 3 測試會發出密碼強度不足警示，或禁止建立、變更通行碼。
(2) 執行步驟 4 測試會發出密碼強度不足警示，或禁止建立、變更通行碼。
(3) 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。
(4) 通過：(1)(2)項結果皆符合，或(3)項結果符合。
(5) 不通過：不滿足(4)的通過條件。
(6) 不適用：產品未支援通行碼鑑別機制。

議題4: 5.2.3.2韌體安全

因應滲透測試的做法出現，暫不考慮韌體僅透過書審來執行

- 問題:
  - 支援FW正確性驗證， 但是不能提供FW簽章工具給實驗室做測試
- 解決方法:
  - 法1: 1級自我宣告；2級才實測。
  - 法2: 請廠商提供安全可信賴的測試環境，例: 實驗室測試期間全程錄影、人員背景正質且為資深員工、電腦無法截圖、不能攜帶拍照錄製設備。

議案5:5.4.3.2連線逾時

- 產品之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。
- 解決方法:
  - 因為持續不間斷的監控是surveillance的正常行為，然而為了同時考量資安的有效性，**因此廠商應於產品使用指南或安全指引，聲明建議的安全做法**。

議案6: 5.5.1.1/5.5.1.2

- 資安需求:
  - ~~5.5.1.2 使用者對其儲存的隱私資料擁有刪除之權限和功能。~~ **(移除)**
- 理由:
  - 實際上在監控領域所錄製的影像，使用者不一定應該要擁有新增、移除、刪除的權限，這比較偏向於消費型的應用。

議案7:新增資料傳送/接收來源測試

5.2.2.1 網路服務最小化測試

(e) 測試方法：

(1) 將測試電腦連接產品。

(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) 目視掃描結果所呈現之網路服務與對應埠。

(4) 比對產品送審資料自我宣告中所聲明之網路服務與對應埠。

/*==========新增==========*/

(5) 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/URL資料

/*==========新增==========*/

臨時動議

- 議題: 晶片資安

Thank you