

影像監控系統資安標準-網路攝影機 (2021) 精要培析

資策會 資安所 副主任
高傳凱 博士





內容修訂摘要

- 安全要求及安全等級只能更嚴格
- 將過去3年廠商產品實務檢測所遇到的問題，調合至新標準中
- 新增全盲滲透測試方法，以填補黑箱檢測方法之不足



實體安全

新舊版差異



5.1.1.1

- 新版強調「若」存在可透過實體介面存取作業系統，才要提供進入作業系統的方法。

備註: 舊版寫法容易讓人誤會一定要提供實體介面進入作業系統的方法，然而這要求最建議的解法是關掉實體介面



系統安全

新舊版差異



5.2.1系列

- 安全1級:

- ◆ 5.2.1.1(a) 系統弱掃

- 安全2級:

- ◆ 5.2.1.1(b) 高權限弱掃

- ◆ 送測廠商應提供系統最高管理(root)權限之帳戶，供實驗室測試用。

- 安全3級:

- ◆ 5.2.1.2 高權限弱掃，且不能掃到CVSS 7.0以上的漏洞



5.2.2.2 遙測資料收集(新增)

- 廠商應提供產品之遙測資料收集與利用宣告作為審查依據(包括但不限於產品使用手冊、包裝說明、本地端管理介面、網頁等介面)。
- 廠商應提供收集遙測資料的伺服器 IP 及/或 URL。
- 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。



5.2.3.1 (軟)韌體更新安全測試

- 明確表明要具備更新功能



5.2.3.2 (原5.2.3.1a) 韌體檔案安全測試

- 狀況1: **韌體檔案加密**之通過條件
 - ◆ 拆解不出檔案系統架構
 - ◆ 審閱可證明所使用加密演算法之 書面資料。
- 狀況2: **韌體檔案未加密**之通過條件
 - ◆ 韌體檔案查找不出金鑰
 - ◆ 韌體檔案查找不出非公開之 email 資料。
 - ◆ 韌體檔案查找不出廠商所宣告相連伺服器外之 IP 資料。
 - ◆ 韌體檔案查找不出廠商所宣告相連伺服器外之 URL 資料



5.2.3.4

韌體更新檔之完整性及真確性測試

● 測試步驟：

◆ 方法 1 (廠商提供測試用私鑰予實驗室)：

- (1) 廠商提供原始韌體並提供簽章方法，實驗室使用自簽私鑰簽署該韌體。
- (2) 實驗室執行韌體更新，檢視更新結果。
- **通過條件:** 實驗室使用自簽私鑰簽署韌體，韌體更新失敗。

◆ 方法 2 (實驗室提供自簽公私鑰予廠商)：

- (1) 實驗室提供自簽公私鑰予送測廠商，廠商利用該私鑰簽署韌體，並將公鑰植 入於產品。
- (2) 實驗室執行韌體更新，檢視更新結果。
- (3) 受測廠商將實驗室所提供之測試私鑰加入受測物之受信任私鑰列表。
- (4) 實驗室執行韌體更新，檢視更新結果。
- **通過條件:** 廠商使用實驗室提供之自簽公私鑰，韌體更新成功。



5.2.4.1 敏感性資料權限管控測試

- 產品不存在作業系統的存取介面，則**不適用**此測項。
- 「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。



5.2.4.2 敏感性資料加密儲存測試 (原1、2級測試整併到1級)

需進入OS

● 前置條件:

- ◆ 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。
- ◆ 應提供產品之系統管理者權限。

● 測試步驟:

- ◆ 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。
- ◆ 檢視產品所儲存之通行碼及加解密用金鑰是否加密保護。



5.2.6 勘誤

條文調整勘誤:

- 5.2.6.1->5.2.6.3
- 5.2.6.2->5.2.6.1
- 5.2.6.3(a)刪除
- 5.2.6.3(b)->5.2.6.2



5.2.6.1 ONVIF

應用程式介面之權限管控機制測試 (勘誤前)

- 前置條件:

- ◆ 產品未啟用 ONVIF profile S，則不適用此測項。



5.2.6.2 ONVIF

應用程式介面之鑑別機制測試 (勘誤前)

- (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。



5.2.7.1 安全事件日誌測試

- 若安全事件日誌為本地儲存，重開機後，該日誌資料仍應存在。
- 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。



5.2.7.4 異常警示功能測試（移除）

- 測試目的：驗證產品是否具有確保安全事件日誌紀錄檔可用性之功能。



通訊安全

新舊版差異



5.3.1.1 敏感性資料之傳輸保護初階測試

5.3.1.2 敏感性資料之傳輸保護中階測試

- 將舊版5.3.1.1拆成5.3.1.1及5.3.1.2，來分別要求安全通道之cipher suite及防止憑證偽冒。
- 除此之外，新增一樣品條件：
 - ◆ 樣品條件：
 - 若與產品對連之影像監控裝置採用自簽發憑證，則產品須提供可編輯中繼憑證之介面



5.4.2.2~5.4.2.4

通行碼強度

● 通過條件：

- ◆ 採用之通行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 無法建立或變更小於8個字元長度之通行碼或產品發出通行碼強度不足警示。
- ◆ 5.4.2.3無法建立或變更通行碼，或產品發出通行碼強度不足警示。



5.4.3.1 權限管控機制

- 通過條件:

- ◆ 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。
- ◆ 例如：產品使用指南告知，產品僅提供單一功能(如：錄影)，無法區分權限。



5.4.3.2 權限有效時間

- 通過條件新增:

- ◆ 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。



舊版5.5.1.2 隱私資料刪除功能

- 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。



5.5.2.1 敏感性資料之傳輸保護初階測試

5.5.2.2 敏感性資料之傳輸保護中階測試

- 將舊版5.5.2.1拆成5.5.2.1及5.5.2.2，來分別要求安全通道之cipher suite及防止憑證偽冒。
- 除此之外，新增一樣品條件：
 - ◆ 樣品條件：
 - 若與產品對連之影像監控裝置採用自簽發憑證，則產品須提供可編輯中繼憑證之介面

Thank you

