影像監控系統資安標準草案–
影像錄影機
(V0.1.0)

推動單位：

台灣資通產業標準協會(TAICS)

制定單位：

台灣資通產業標準協會之網路與資訊安全技術工作委員會(TC5)

支持單位：

經濟部工業局、財團法人資訊工業策進會

2017-09-05

文件修改記錄

版本	修改日期	修改人	問題單流水號	修改原因及說明
V0.1.0	2017/9/5	陳聰杰	無	新建立

目錄

前言

物聯網科技是全世界發展最快速的產業，相關應用不斷推陳出新，而物聯網科技成功與否，資訊安全是最主要的關鍵，因此經濟部工業局率先提出制定物聯網資安法制環境的目標，包括物聯網通用資安標準、輔助應用程式資安標準、影像監控系統資安標準、工控系統資安標準、車聯網系統資安標準、醫療儀器資安標準及銷售點終端系統資安標準，全面推升國內資安產業自主研發能量，提供穩定且安全的產業發展環境。

物聯網的盛行，使日常用品皆朝向網路化邁進，影像錄影機也是其中之一，運用範圍包括：影音預覽、錄影錄音、影音回放、資料備份、遠端監控服務等，相當受到消費者青睞，但隨之而來的問題是網路攻擊事件，從 2014 年起網路資安事件日益頻繁、攻擊事件規模越來越大，2016 年底以 Mirai 為名的惡意程式，藉由影像錄影機為跳板，製造出前所未聞之網路攻擊的手法。

有鑑於此，藉由「影像監控系統資安標準草案-影像錄影機」之制定(以下簡稱本標準)，建立國內在確保影像錄影機資安品質的規範，期使設備商或系統服務商在產品研發上有所依據，促進國內產業整體優質化及產品競爭力，確保消費者在影像錄影機之運用上達到安全的目的。

本標準之制定係參照國際物聯網相關資安標準/規範，如 ISO 27001[2]、UL 2900 系列標準[7]、GSMA IoT Security Guideline[1]、OWASP Top IoT Vulnerabilities[6]及日本政府的物聯網安全指導方針[10]等，主要規劃從六大面向確保影像錄影機的資訊安全，包括實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護及應用程式安全；並分成三個安全需求等級，詳盡載明欲實踐每一個安全需求等級的必要條件，用以界定不同產品須具備之資安要求。

在確保影像錄影機的資安品質時，應同時考量整體影像監控系統的安全性，例如:管理影像錄影機的雲服務被駭客入侵、操控影像錄影機的行動應用程式含有軟體漏洞及安全等級不足的網路攝影機等因素，皆可能對影像錄影機造成資安威脅，因此建議設置時時須參閱所有相關產品之資安標準，達到整體網路影像監控系統的安全保證(Security Assurance)。

1. 適用範圍

泛指應用於影像監控系統的影像錄影機，且凡是影像錄影機本身具連網功能者皆是影像錄影機的一種，如圖 1 實線框處所示。

本標準為確保影像錄影機資安，訂定其產品之安全技術要求，擬分為六大面向做為評測要項，包括：實體安全、系統安全、通訊安全、身分認證與授權機制安全、隱私保護及應用程式安全。

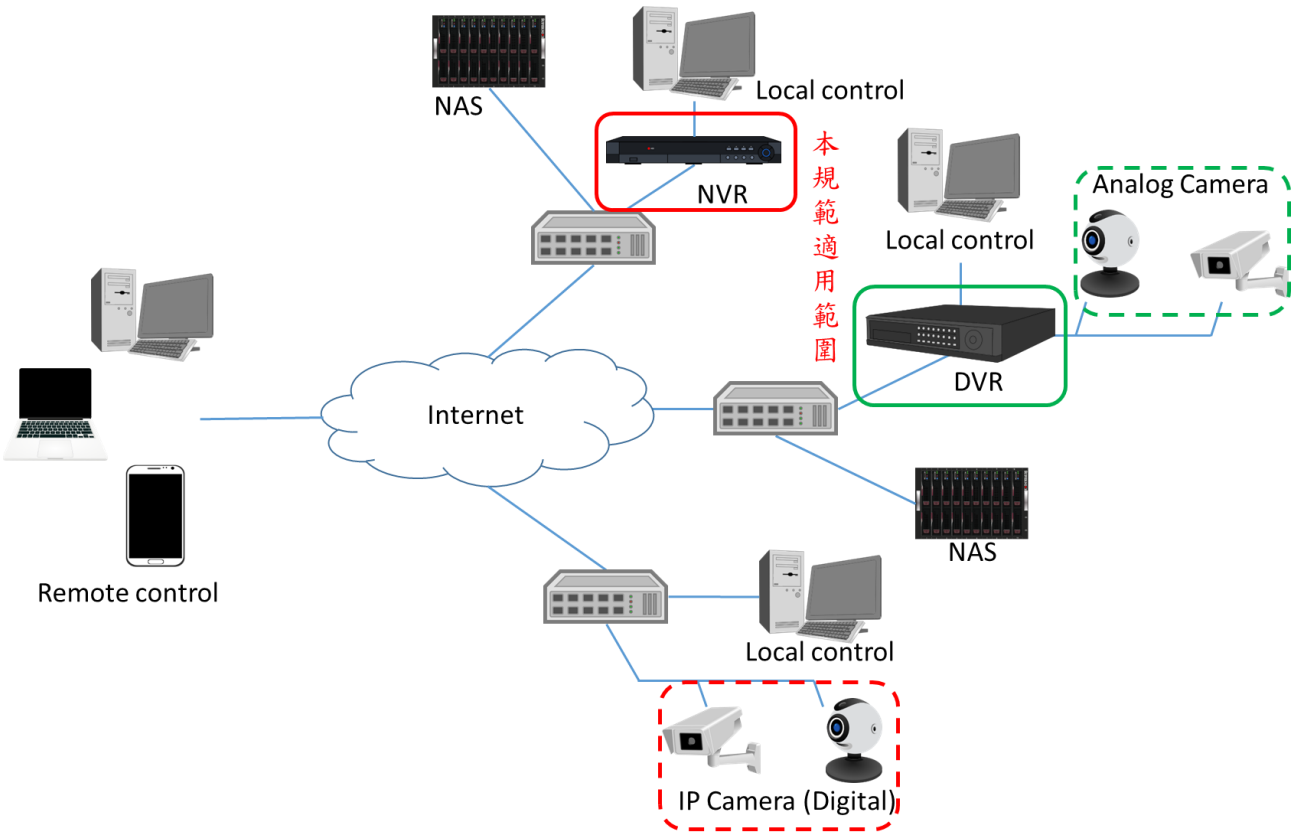

圖 1 適用範圍示意圖

2. 用語及定義

下列用語與定義適用於本標準。

2.1 影像錄影機 (Video Recoder)

係指一種主要用於影像監控系統且具連網功能的影像錄影機，其應用類型包括：數位影像錄影機（Digital Video Recorder，DVR）與網路影像錄影機(Network Video Recorder, NVR)等。

2.2 資訊安全弱點 (Security Vulnerability)

指受測裝置安全方面之缺陷，使得系統或行動應用程式資料之保密性、完整性及可用性面臨威脅。

2.3 常見弱點與漏洞 (Common Vulnerabilities and Exposures , CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號。

2.4 已知安全性弱點（Known Security Vulnerabilities）

係指 2.3 常見弱點與漏洞中各編號之漏洞。

2.5 國家資安弱點資料庫 (National Vulnerabilities Database)

係指美國國家標準技術研究所（NIST）提供的國家資安弱點資料庫[3]，負責 2.3 常見弱點與漏洞之資料的發布及更新。

2.6 敏感性資料 (Sensitivity Data)

指依使用者行為或行動應用程式之運作，於裝置及其附屬儲存媒介建立、儲存或傳輸之資訊，而該資訊之洩漏可能對使用者造成損害之虞，包括但不限於個人資料、密碼或地理位置等。

2.7 個人資料 (Personally Identifiable Information)

指主要依「個人資料保護法」上定義之所有得以直接或間接方式識別該個人之資料，包括自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

2.8 隱私 (Privacy)

係指私人資訊，此一資訊的全部或部份不可被公開，且所有人有權利去保護的部分，本標準所指之隱私包括影像錄影機所錄製之影像及用戶資訊。

2.9 遠端管理介面 (Remote Control Management, RCM)

係指透過網路自遠端裝置上取得影像錄影機作業系統層的操控權，作業模式如下列：

(a) 工程師遠端維護產品使用或透過網頁管理介面遠端存取影像錄影機資源，例如：監看畫面、操控鏡頭

(b) 進行系統設定，例如：設定**網際協定位址**(IP)。

2.10 操控程式 (Control Program)

係指用於控制影像錄影機行為或瀏覽監控內容之應用程式，目前可能的應用程式類型包括行動版及電腦版。

2.11 應用程式介面 (Application Program Interface, API)

係指軟體系統不同組成部分銜接的約定。大部份影像錄影機皆提供 API 給操控端之應用程式呼叫，用戶可透過這些 API，撰寫實際實現影像錄影機相關操作(例如：系統資訊擷取、監控影像擷取等)的應用程式。

2.12 第三方函式庫 (3rd Party Library)

係指系統程式設計者為加速開發，引用其他組織所製作具備某特定功能之函式庫，以滿足裝置所需提供的服務。

2.13 加密 (Encryption)

係指明文資訊透過數學演算法進行改變，使原來的資料不可讀而達到保密的目的。

2.14 數位簽章 (Digital Signature)

係指簽署人以私鑰簽名經由數學演算法處理過後產生一定長度之電子文件，形成電子簽章，並得以公開金鑰進行驗證，不僅可確保該文件的完整性，同時驗證文件作者的不可否認性。

2.15 安全通道 (Security Tunnel)

目的是為網際網路通訊的端點與端點(End-to-End)之間，建立一條兼顧資料隱密性及完整性之通道，目前常見之實作通訊協定為安全通訊端層(SSL)和傳輸層安全性(TLS)。

2.16 安全區域 (Secure Domain)

係指與正常作業環境隔離出的區域，僅用於執行安全性相關操作，如：加解密、金鑰管理、完整性檢查，並保存敏感性資料用。

2.17 密碼 (Password)

係指一組字元串能讓系統辨識用戶身分，並可進一步控管用戶存取系統之權限。

2.18 預設密碼 (Default Password)

係指產品在用戶初次將其連上網路，且在未更改任何設定的情況下，用以登入影像錄影機之密碼。

3. 安全保證等級

本標準旨在建立評估及驗證時所遵循的共同標準，判定產品之安全保證等級。安全保證係指為降低或消弭資訊產品之安全威脅，選擇合適之安全保證組合，確保產品達到安全保證之要求。

安全保證分級依(1)檢測所需時間、(2)安全技術深度、(3)目前尚無通用檢測方法、(4)產品技術現況等驗證項目，共分為三等級，並依等級順序排列，越高表示安全保證等級越高。

安全保證分級總表如表 1 所示，依據五大安全面向分別設計對應之安全要求分類，再依各安全要求分類之實地驗證評估安全保證等級：

(a) 實體安全：從產品是否能輕易被拆解，或產品之儲存與測試除錯用之連接埠的管控，作為建立安全要求的標的。

(b) 系統安全：檢視產品之作業系統、網路服務、更新服務及軟韌體程式設計等，是否具備足夠之安全防護。

(c) 通訊安全：著重在機敏資料之通訊安全，和探查通訊服務是否存在未知之資安漏洞。

(d) 身分認證與授權機制安全：影像錄影機存在數種不同的溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，無論從那一類介面，皆須確保認證與授權機制的落實。

(e) 隱私保護：影像錄影機之隱私，包括使用者之資料和影像、儲存與傳輸的保護及權限管控等，確保隱私資料不外洩。

(f) 應用程式安全：影像錄影機之應用程式安全包括出廠預載軟體、銷售商加載軟體及無圖示軟體 3 種屬性，以確保其符合現階段資訊安全要求，但不包含使用者自行下載之非原廠軟體或附加服務。

表 1 依據五大安全面向分別設計對應之安全要求分類，每一安全要求分類包含一個以上之安全要求，1 級、2 級、3 級三欄表示安全保證等級之區分，係與其對應之列代表的安全技術要求分類，識別一個特定的技術要求。

表 1 安全要求保證等級總表

安全面向	安全要求分類	安全保證分級		
		一級	二級	三級
實體安全	4.1.1. 實體埠之安全管控	4.1.1.1	4.1.1.2	4.1.1.2
	4.1.2. 實體異常行為警示		4.1.2.1	4.1.2.1
	4.1.3. 實體防護		4.1.3.1	4.1.3.2
	4.1.4. 安全啟動			4.1.4.1
系統安全	4.2.1. 作業系統安全	4.2.1.1	4.2.1.2	4.2.1.3
	4.2.2. 網路服務連接埠	4.2.2.1	4.2.2.1	4.2.2.1
	4.2.3. 網路服務安全	4.2.3.1	4.2.3.2	4.2.3.3
	4.2.4. 更新安全	4.2.4.1	4.2.4.2	4.2.4.2
	4.2.5. 軟韌體程式安全	4.2.5.1	4.2.5.1	4.2.5.2
	4.2.6. 敏感性資料儲存安全	4.2.6.1	4.2.6.1	4.2.6.2
	4.2.7. 網頁管理介面安全	4.2.7.1	4.2.7.1	4.2.7.1
	4.2.8. 操控程式之 API 安全	4.2.8.1	4.2.8.1	4.2.8.2
	4.2.9. 系統日誌檔與警示	4.2.9.1	4.2.9.2	4.2.9.2
通訊安全	4.3.1. 敏感性資料傳輸安全	4.3.1.1	4.3.1.1	4.3.1.2
	4.3.2. 通訊介面的安全設置	4.3.2.1	4.3.2.1	4.3.2.1
	4.3.3. 通訊協定安全		4.3.3.1	4.3.3.1
身分認證與授權機制安全	4.4.1. 認證機制安全	4.4.1.1	4.4.1.1	4.4.1.2
	4.4.2. 密碼認證機制	4.4.2.1	4.4.2.1	4.4.2.1
	4.4.3. 權限控管	4.4.3.1	4.4.3.1	4.4.3.1
隱私保護	4.5.1. 隱私資料的存取保護	4.5.1.1	4.5.1.1	4.5.1.1
	4.5.2. 隱私資料的傳輸保護	4.5.2.1	4.5.2.2	4.5.2.3
應用程式安全	4.6.1. 應用程式的程式安全	4.6.1.1	4.6.1.2	4.6.1.3
	4.6.2. 應用程式的系統安全	4.6.2.1	4.6.2.2	4.6.2.3

3.1.1 安全保證第一級

係指產品的功能及操作上主要以便利性為導向，安全威脅則是次要考量的應用環境，然而專注於必須保護的敏感資料及個人資料的管控，是開發商對於用戶提供最基本的安全保證。

表 2　第一級安全技術要求

安全類別	安全技術要求
實體安全	4.1.1.1 出廠之實體埠必須具備安全管控。
系統安全	4.2.1.1 作業系統不得存在 CVSS v3 評分為 10 分之資訊安全漏洞
	4.2.2.1 產品啟用之網路服務須與廠商自我聲明之一致
	4.2.3.1 網路服務不得存在 CVSS v3 評分為 10 分之資訊安全漏洞
	4.2.4.1 軟韌體更新機密性保證
	4.2.5.1 產品之敏感性資料不得出現於裝置軟韌體程式碼中
	4.2.6.1 產品所儲存之敏感性資料須透過加密儲存
	4.2.7.1 網頁管理介面不得存在 OWASP top 10 [5]中所揭露之常見網站安全風險
	4.2.8.1. API 之認證機制強度
	4.2.9.1 產品須提供安全事件日誌檔
通訊安全	4.3.1.1 敏感資料於傳輸過程中須加密保護
	4.3.2.1 避免錯誤的通訊介面設置
身分認證與授權機制安全	4.4.1.1 認證機制強度
	4.4.2.1 密碼認證機制強度
	4.4.3.1 影像錄影機資源的存取，必須具備權限管控機制
隱私保護	4.5.1.1 隱私資料的權限管控
	4.5.2.1 隱私資料傳輸機密性之基本要求
應用程式安全	4.6.1.1 應用程式的程式安全之基本要求。
	4.6.2.1 應用程式的系統安全之基本要求。

3.1.2 安全保證第二級

組織在營運規劃上考量資安重要性，且欲於良好商業發展活動上，積極發展安全工程技術，期望獲得最大保證，是準備付出額外的安全工程，但不須大幅度重新設計開發。

表 3. 第二級安全技術要求

安全類別	安全技術要求
實體安全	4.1.1.2 除達到 4.1.1.1 要求外，產品的外觀不得有實體埠存在
	4.1.2.1 影像錄影機之硬體設計須具備異常狀態之警示機制
	4.1.3.1 產品之外殼不能被輕易拆除或破壞
系統安全	4.2.1.2 作業系統不得存在 CVSS v3 評分為 9 分之資訊安全漏洞
	4.2.2.1 產品啟用之網路服務須與廠商自我聲明之一致
	4.2.3.2 網路服務不得存在 CVSS v3 評分為 9 分之資訊安全漏洞
	4.2.4.2 軟韌體更新機制強度
	4.2.5.1 產品之敏感性資料不得出現於裝置軟韌體程式碼中
	4.2.6.1 產品所儲存之敏感性資料須透過加密儲存
	4.2.7.1 網頁管理介面不得存在 OWASP top 10 [5]中所揭露之常見網站安全風險
	4.2.8.1. API 之認證機制強度
	4.2.9.2 產品須提供異常警示功能
通訊安全	4.3.1.1 敏感資料於傳輸過程中須加密保護
	4.3.2.1 避免錯誤的通訊介面設置
	4.3.3.1 影像錄影機所使用之關鍵通訊協定(見附錄 A)，必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。
身分認證與授權機制安全	4.4.1.1 認證機制強度
	4.4.2.1 密碼認證機制強度
	4.4.3.1 影像錄影機資源的存取，必須具備權限管控機制
隱私保護	4.5.1.1 隱私資料的權限管控

	4.5.2.2 隱私資料傳輸機密性之進階要求
應用程式安全	4.6.1.2 應用程式的程式安全之進階要求。
	4.6.2.2 應用程式的系統安全之進階要求。

3.1.3 安全保證第三級

應用環境屬於高風險情況時，願為保護資產之價值使額外付出顯得正當時，以保護高價值資產對抗高風險為最終目的。開發者為獲得較高安全保證，需透過安全工程技術應用，且大幅度的重新設計開發。

表 4 第三級安全技術要求

安全類別	安全技術要求
實體安全	4.1.1.2 除達到 4.1.1.1 要求外，產品的外觀不得有實體埠存在
	4.1.2.1 影像錄影機之硬體設計須具備異常狀態之警示機制
	4.1.3.2 避免不安全的實體設計
	4.1.4.1 產品須提供安全啟動(secure boot)功能
系統安全	4.2.1.3 作業系統不得存在 CVSS v3 評分為 7 分之資訊安全漏洞
	4.2.2.1 產品啟用之網路服務須與廠商自我聲明之一致
	4.2.3.3 網路服務不得存在 CVSS v3 評分為 7 分之資訊安全漏洞
	4.2.4.2 軟韌體更新機制強度
	4.2.5.2 除達到 4.2.5.1 要求外，產品的軟韌體不得存在因程式設計錯誤，而導致程式存在安全性弱點
	4.2.6.2 敏感資料的存放，須從正常作業環境中隔離。
	4.2.7.1 網頁管理介面不得存在 OWASP top 10 [5]中所揭露之常見網站安全風險
	4.2.8.2 操控程式之 API 必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形
	4.2.9.2 產品須提供異常警示功能
通訊安全	4.3.1.2. 敏感性資料傳輸須採用較嚴謹之加密演算法，且須確保敏

	感性資料傳輸的完整性及不可否認性
	4.3.2.1 避免錯誤的通訊介面設置
	4.3.3.1 影像錄影機所使用之關鍵通訊協定(見附錄 A)，必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。
身分認證與授權機制安全	4.4.1.2 嚴謹之認證機制要求。
	4.4.2.1 密碼認證機制強度
	4.4.3.1 影像錄影機資源的存取，必須具備權限管控機制
隱私保護	4.5.1.1 隱私資料的權限管控
	4.5.2.3 隱私資料傳輸機密性之高階要求
應用程式安全	4.6.1.3 應用程式的程式安全之高階要求。
	4.6.2.3 應用程式的系統安全之高階要求。

4. 標準規範

4.1 實體安全

4.1.1 實體埠之安全管控

4.1.1.1 出廠之實體埠必須具備安全管控。

A. 在實體埠的安全管控上，不得被利用來存取產品之作業系統。

B. 實體埠採最小數量使用原則，沒使用到的實體埠可以被關閉，即用於除錯和測試及外接儲存媒體用功能必須關閉。

C. 外接實體埠的插拔操作須提供日誌記錄。

4.1.1.2 產品不得有外接儲存用及除錯測試用之實體介面存在。

A. 所有不使用的介面應移除，包括外接式儲存媒體使用的插槽、電路板上用於除錯或測試用途之界面，必須移除。

4.1.2 實體異常行為警示

4.1.2.1. 影像錄影機之硬體設計須具備異常狀態之警示機制。

A. 產品於實體操作出現異常時須提供警示機制，包括：鏡頭被異物遮敝時、實體設備遭竊取時或實體設備遭受破壞時，例如：機殼、元件被拆除。

B. 實體設計之自動化硬體偵測機制，包括：剪線發報機制、前置錄影、位移偵測、斷電復歸、準位偵測功能等，須提供警示機制，例如：E- Mail 通知、訊息推播、蜂鳴器等。

4.1.3 實體防護

4.1.3.1 產品之外殼不能被輕易拆除或破壞。

A. 產品在實體上要有防止被輕易拆除或破壞之設計護，可能的做法是產品之外殼應該使用鐵殼來增加被暴力破壞的難度，或者是透過防盜螺絲來迫使拆解變得更加困難。

4.1.3.2 避免不安全的實體設計。

A. 除達到 4.1.3.1 要求外，晶片與功能編號不得存在於電路板。

B. 除達到 4.1.3.1 要求外，產品實體上不得存在可輕易一鍵還原回預設密碼的設計，即不須透過任何工具，可輕易在產品實體上一鍵還原回預設密碼須避免。

4.1.4 安全啟動

4.1.4.1 產品須提供安全啟動(secure boot)功能。

A. 確保產品於開機時，避免未經授權的軟韌體、驅動程式及作業系統的執行，一旦系統的完整性及可信度獲得保證，產品始得開機。

4.2 系統安全技術要求

4.2.1 作業系統安全

4.2.1.1 作業系統不得存在 CVSS v3 評分為 10 分之資訊安全弱點。

A. 受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 10 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.1.2 作業系統不得存在 CVSS v3 評分為 9 分之資訊安全弱點。

A. 受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.1.3 作業系統不得存在 CVSS v3 評分為 7 分之資訊安全弱點。

A. 受測產品之作業系統，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.2 網路服務連接埠

4.2.2.1 影像錄影機僅開啟必要之網路服務。

A. 開啟之網路服務僅須為廠商提供必要服務之所需，透過最小化網路服務之啟用，即可降低產品的可入侵介面，廠商須於文件中標明所啟用之服務，以確保是否存在未宣告之網路服務連接埠被開啟。

4.2.3 網路服務安全

4.2.3.1 網路服務不得存在 CVSS v3 評分為 10 分之資訊安全漏洞。

A. 受測產品之網路服務，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 10 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.3.2 網路服務不得存在 CVSS v3 評分為 9 分之資訊安全漏洞。

A. 受測產品之網路服務，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 9 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.3.3 網路服務不得存在 CVSS v3 評分為 7 分之資訊安全漏洞。

A. 受測產品之網路服務，不得存在國家弱點資料庫[3]所公開的常見弱點與漏洞資料，且 CVSS v3 評分為 7 分，包括不得存在已經公開的攻擊程式碼、實際攻擊案例、概念性驗證攻擊手法或漏洞之技術分析。

4.2.4 更新安全

4.2.4.1 軟韌體更新機密性保證。

A. 軟韌體須具備更新機制。

B. 產品支援離線手動更新，則更新檔案得確保機密性，且使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[4]。

C. 產品支援線上更新，則更新路徑得通過安全通道，且安全通道必須是 TLS 1.1 以上，以及使用之加密演算法須採用 FIPS 140-2 所核可之加密演算法[4]。

4.2.4.2 軟韌體更新機制強度。

A. 除達到 4.2.4.1 要求外，軟韌體更新機制須一律採用線上更新。

B. 除達到 4.2.4.1 要求外，軟韌體更新必須透過數位簽章機制確保更新檔案的完整性及可信度。

4.2.5 軟韌體程式安全

4.2.5.1 產品之敏感性資料不得出現於裝置軟韌體程式碼中。

A. 產品之帳號、密碼、身分認證因子或加解密用之金鑰，不得出現於軟韌體之程式碼與安裝檔內其他檔案中。

4.2.5.2 除達到 4.2.5.1 要求外，產品的軟韌體不得存在因程式設計錯誤，而導致程式存在安全性弱點。

A. 產品的軟韌體不得存在 CWE/SANS TOP 25 Most Dangerous Software Errors [11]。

4.2.6 敏感性資料儲存安全

4.2.6.1 產品所儲存之敏感性資料須透過加密儲存。

A. 產品之敏感性資料須透過加密儲存，必須使用 FIPS 140-2 所核可之加密演算法[4]確保機密性。

4.2.6.2 敏感資料的存放，須從正常作業環境中隔離。

A. 敏感資料必須存放於產品的安全區域(Secure domain)中。

4.2.7 網頁管理介面安全

4.2.7.1 網頁管理介面不得存在 OWASP top 10 [5]中所揭露之常見網站安全風險。

A. 確保產品本身提供之網頁管理介面不得存在 OWASP top 10 之 A1-Injection 及 A3-Cross-Site Scripting (XSS)攻擊。

4.2.8 操控程式之 API 安全

4.2.8.1 API 之認證機制強度。

A. API 之身分認證機制，不得因為重送攻擊(Replay Attack)而使得認證被通過。

B. 認證錯誤訊息不能顯露出合法使用者名稱。

C. 參照 FIPS SP 800-63-3[8] 密碼強度原則，密碼認證機制之密碼長度必須支援 15 個字母長度。

D. 廠商所生產之影像錄影機其預設密碼都須相異。

E. 首次成功取得影像錄影機 API 之認證，必須強制更改預設密碼。

F. 產品在認證密碼的設計上必須有輸入頻率及次數的限制。

G. API 的存取，必須具備權限管控機制，產品須將使用者角色切割成數個使用者環境，例如：一般使用者、特權使用者、系統管理者等，並於文件中標明現存角色與其對應的權限，以確保產品之角色權限與廠商所宣告相符。

H. 產品之授權行為，應存在閒置時限供使用者設定。

4.2.8.2 操控程式之 API 必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

A. 透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免 API 因為任意或非法的輸入，造成產品異常行為的發生。

4.2.9 系統日誌檔與警示

4.2.9.1 產品須提供安全事件日誌檔。

A. 須具備安全事件日誌檔之顯示功能，以記錄用戶的存取行為，用以察覺未授權或異常的登入操作，產品須提供完整時間戳記、使用者身分及操作行為之安全事件日誌檔供查閱。

B. 產品之安全事件日誌檔須具備權限控管機制，該紀錄檔不得允許未經授權的修改，以防止被竄改的可能。

C. 產品之安全事件日誌檔紀錄檔須具備顯示功能機制。

4.2.9.2 產品須提供異常警示功能。

A. 除達到 4.2.9.1 要求外，產品須提供異常警示功能。

B. 除達到 4.2.9.1 要求外,影像錄影機應提供當日誌紀錄檔無法儲存時之系統警示。

4.3 通訊安全技術要求

4.3.1 敏感性資料傳輸安全

4.3.1.1 敏感資料於傳輸過程中須加密保護。

A. 敏感資料之網路傳輸必須使用 FIPS 140-2 所核可之加密演算法[4]，以確保機密性。

4.3.1.2. 敏感性資料傳輸須採用較嚴謹之加密演算法，且須確保敏感性資料傳輸的完整性及不可否認性。

A. 確保敏感資料之網路傳輸加密演算法必須支援 AES-256。

4.3.2 通訊介面的安全設置

4.3.2.1 避免錯誤的通訊介面設置

A. 產品須提供用戶可自行開/關「網路裝置資訊探詢」功能，例如：UPnP、SNMP 及 Bonjour，且預設須為關閉狀態。

B. 產品須提供用戶可自行開/關無線網路之 WPS PIN 及 WPS Lock 功能，且預設為須為關閉。

C. 無線網路傳輸的安全機制預設必須採用 WPA2。

4.3.3 通訊協定安全

4.3.3.1 影像錄影機所使用之關鍵通訊協定，必須經過異常輸入檢測，不得發生崩潰(crash)導致服務中止的情形。

A. 透過錯誤處理漏洞的查找，包括檢視訊息長度、訊息 ID 及關鍵協定屬性等欄位，避免關鍵之通訊協定(見附錄 A)因為任意或非法的輸入，造成產品異常行為的發生。

4.4 身分認證與授權機制安全技術要求

4.4.1 認證機制安全

4.4.1.1 認證機制強度-初階。

A. 產品之身分認證機制，不得因為重送攻擊而使得認證被通過。

B. 認證錯誤訊息不能顯露出合法使用者名稱。

4.4.1.2 認證機制要求-高階。

A. 除達到 4.4.1.1 要求外，產品之身分認證機制須採用公開金鑰基礎建設。

B. 除達到 4.4.1.1 要求外，產品之身分認證機制須採用雙向認證機制。

4.4.2 密碼認證安全

4.4.2.1 密碼認證機制強度。

A. 參照 FIPS SP 800-63-3[8] 密碼強度原則，密碼認證機制之密碼長度必須支援 15 個字母。

B. 廠商所生產之影像錄影機其預設密碼都須相異。

C. 首次登入產品必須強制更改預設密碼。

D. 產品在登入密碼的設計上必須有輸入頻率及次數的限制。

4.4.3 權限管控

4.4.3.1 影像錄影機資源的存取，必須具備權限管控機制。

A. 產品須將使用者角色切割成數個使用者環境，例如：一般使用者、特權使用者、系統管理者等，並於文件中標明現存角色與其對應的權限，以確保產品之角色權限與廠商所宣告相符。

B. 對所有合法授權之帳戶強制實施最小權限(least privilege)原則，此外，系統管理者有其專門的特權，其它角色不能擁有這樣的權限。

C. 產品之授權行為，應存在閒置時限供使用者設定，一旦遠端連線已經遺失或結束，須要求新的認證。

4.5 隱私保護技術要求

4.5.1 隱私資料的存取保護

4.5.1.1 隱私資料的權限管控

A. 產品所儲存的隱私資料，只有已被授權的個體才可以存取。

B. 具備使用者刪除其隱私資料之功能，及對所儲存隱私資料的刪除權限。

4.5.2 隱私資料的傳輸保護

4.5.2.1 隱私資料傳輸機密性之基本要求。

A. 影像類隱私資料之傳輸不得為明文，非影像類隱私資料之傳輸，須使用 FIPS 140-2 所核可之加密演算法[4]。

4.5.2.2 隱私資料傳輸機密性之進階要求。

A. 隱私資料之傳輸須使用 FIPS 140-2 所核可之加密演算法[4]。

4.5.2.3 隱私資料傳輸機密性之高階要求。

A. 確保隱私資料之網路傳輸加密演算法預設必須採用 AES-256。

4.6 應用程式技術要求

4.6.1 應用程式的程式安全

4.6.1.1 應用程式的程式安全之基本要求

A. 應用程式在初次存取使用者已綁定裝置之帳戶時，應先行認證使用者身分與其權限，以避免使用者帳戶遭誤用或濫用。

B. 應用程式應確認資料來源的安全。

C. 應用程式應可識別其發行資訊，以確保使用者瞭解其來源。

D. 應用程式所執行的行為，應取得使用者同意，並與其宣告之內容相符。

E. 應用程式所開啟之網路連接埠須與「廠商自我宣告表」所宣告之「網路埠」相符。

F. 廠商需於文件中標明所使用之應用程式及引用之第三方函式庫。

G. 應用程式所引用之第三方函式庫，不得存在已揭露之重大資訊安全漏洞。

H. 應用程式必須具備應用程式更新機制。

I. 應用程式之敏感性資料不得出現於裝置應用程式程式碼中。

4.6.1.2 應用程式的程式安全之進階要求

A. 應用程式不應在未取得使用者同意之情況下，於背景發送簡訊。

B. 應用程式於使用者設定關閉時，應停止該內建軟體所有相關程序。

C. 應用程式可能有程式設計上缺陷，內建應用程式應經過源碼掃描。

4.6.1.3 應用程式的程式安全之高階要求

A. 應用程式應具備惡意字串輸入時的處理能力。

B. 應用程式應提供回報安全性問題之管道。

C. 應用程式可能被竄改，內建應用程式須具備數位簽章。

4.6.2 應用程式的系統安全

4.6.2.1 應用程式的系統安全之基本要求

A. 應用程式所執行的程式行為，應取得使用者同意，必要時並提供風險提示。

B. 應用程式於下載或安裝更新作業系統時應提供更新通知，並告知使用者安全風險之資訊。

C. 應用程式應提供安全的身分辨識及保護機制。

4.6.2.2 應用程式的系統安全之進階要求

A. 應用程式應支援螢幕解鎖保護機制，以保護個人資訊避免遭未經授權的使用。

B. 應用程式應支援螢幕解鎖錯誤之強制鎖定保護機制，以保護個人資訊，避免遭未經授權的使用。

C. 應用程式之螢幕鎖定解鎖資料，不應以明文方式儲存，以避免遭未經授權的使用。

D. 參照 FIPS SP 800-63-3[8] 密碼強度原則，密碼認證機制之密碼長度至少須 15 個字母。

E. 應用程式應提供回報安全性問題之管道。

4.6.2.3 應用程式的系統安全之高階要求

A. 應用程式應建立與通訊目標間受信任的傳輸通道,作為傳輸期間資料保護使用。

B. 開機過程應提供密碼功能測試與系統軟體完整性自我測試機制。

C. 應用程式須提供讓安全應用程式執行之安全區域。

D. 應用程式須具備應用程式異常操作之監控及防護。

附錄 A

(規定)

影像錄影機所使用之通訊協定

A.1 即時傳輸協定 (Real-time Transport Protocol, RTP)：

定義在 RFC 3550 規範中，常應用於影音串流(Video Streaming)系統、視訊會議及一鍵通(Push to Talk)系統，其定義了在網際網路上傳遞音訊和影片的標準封包格式。

A.2 即時傳送控制協定 (Real-time Transport Control Protocol, RTCP)：

定義在 RFC 3550 規範中，RTCP 並不用於資料傳輸，而是支援 RTP 將多媒體資料封裝並發送，RTCP 會週期性地在一個 RTP 會議連線上以帶外(out-of-band)的方式提供統計及傳輸控制資訊，此協定之主要功能是為 RTP 提供服務品質(Quality of Service)的反饋(feedback)。

A.3 即時串流協定 (Real Time Streaming Protocol, RTSP)：

定義在 RFC 2326 規範中，用來控制具有即時性需求的資料，如影音多媒體資料的播放、錄製及暫停，可達到用戶端到媒體伺服器之間的即時影音控制。

A.4 超文本傳輸協定(HyperText Transfer Protocol, HTTP)：

定義在 RFC 7540 規範中，超文本傳輸協定之全名為 HypertText Transfer Protocol（簡稱為 HTTP），是目前網際網路上應用最廣泛的一個網路協議（protocol），其主要目的是為了提供網頁的發佈與取得。

A.5 HTTPS 加密協定(HyperText Transfer Protocol Secure, HTTPS)：

定義在 RFC 2818 規範中，是一種經由 HTTP 進行通訊傳輸，且傳輸是建立在 SSL/TLS 安全通道之上，以保護傳輸中之資料。HTTPS 的主要應用是對網站伺服器進行身分認證，確保傳輸中資料的隱密性與完整性。

A.6 乙太網路點對點通訊協定(Point-to-Point Protocol Over Ethernet, PPPoE)：

定義在 RFC 2818 規範中，是一種經由 HTTP 進行通訊傳輸，且傳輸是建立在 SSL/TLS 安全通道之上，以保護傳輸中之資料。HTTPS 的主要應用是對網站伺服器進行身分認證，確保傳輸中資料的隱密性與完整性。

A.7 動態功能變數名稱服務(Dynamic Domain Name Server, DDNS)：

定義在 RFC 2136 規範中，是一種自動更新名稱伺服器（Name server）內容的技術，提供浮動 IP 或非固定(DHCP)IP 的主機可以動態 IP 地址映射之功能。

參考資料

1. GSMA corp., IoT Security Guidelines for Endpoint Ecosystems
2. CNS 27001 資訊技術－安全技術－資訊安全管理系統－要求事項
3. NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing
4. NIST, Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017
5. OWASP.org, OWASP Top Ten 2017 Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
6. OWASP.org, Top IoT Vulnerabilities, https://www.owasp.org/index.php/Top_IoT_Vulnerabilities
7. UL 2900-1, Outline of Investigation for Software Cybersecurity for Network Connectable Products, Part 1: General Requirements
8. NIST, NIST Special Publication 800-63-3: Digital Identity Guidelines, June, 2017
9. 行動應用資安聯盟, 行動應用 App 基本資安規範 V1.1
10. 總務省･經濟產業省, IoT セキュリティガイドライン ver 1.0
11. MITRE, 2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/