TAICS

TAICS TS-0049 v1.0 : 2022

數據機資安標準

Cybersecurity standard for modem

2022/09/15

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

數據機資安標準

Cybersecurity standard for modem

出版日期: 2022/09/15

終審日期: 2022/08/09

誌謝

本標準由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC 主席：神盾股份有限公司 張心玲 副總經理

TC 副主席：財團法人電信技術中心 林炫佑 副執行長

TC 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人電信技術中心 王慶豐 副主任、許博堯 副理、張彥威 工程師

此標準制定之協會會員參與名單為(以中文名稱順序排列)：

中華資安國際股份有限公司、中華電信股份有限公司、合勤科技股份有限公司、安華聯網科技股份有限公司、亞旭電腦股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人台灣商品檢測驗證中心、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、智邦科技股份有限公司、智易科技股份有限公司、遠傳電信股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

國立雲林科技大學、凱擘股份有限公司

本標準由國家通訊傳播委員會支持研究制定

目錄

前言

本標準係依台灣資通產業標準協會(TAICS)之規定，經理事會審定，由協會公布之產業標準。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

數據機(Modem) 泛指對通信設備所傳輸訊號進行調變或解調的設備，能於傳送時將資料處理設備相容的資料形式調變為與傳輸設備相容的資料形式，且於接收時進行反向的解調轉換。常見的數據機包含固網數據機(xDSL、撥接上網等方式)、行動連網裝置(4G/5G/Wi-Fi 等方式)等等，可將無線電波、光纖網路/電纜線脈衝訊號，經由 modem 轉化為數位訊號，提供與數據機串接的路由器、閘道、行動裝置等連網裝置，連接成彼此能互相通信的網路。

數據機也成為常見的惡意網路攻擊媒介與破口，駭客除了對數據機發動攻擊或攔截訊號以外，也會盜取或側錄與數據機串接的內網連網裝置關鍵資料及參數，造成對數據機本身架構安全性，甚至是數據機與連網裝置持有者隱私的衝擊，例如 CVE-2019-13411 便發現數據機在 3097 埠可以遠端執行任意指令，CVE-2019-13412 則可以利用來讀取任意文件，CVE-2019-15064 則可以讓攻擊者無需任何身分驗證即可登錄設備，CVE-2019-15065 則可以允許攻擊者在 6998 埠上執行特定命令來讀取內容。

本標準制定之目的為增進數據機安全功能，並導入資安防護設計概念與技術，保障數據機運作安全性與資料完整性。

1. 適用範圍

本標準規定數據機之資訊安全要求。數據機(modem)為連接使用者終端設備至ISP業者間之提供上網功能設備，如圖 1 所示。本標準之適用範圍為數據機本體，包括硬體、韌體、輸出入介面、傳輸協定等，與圖 2 所示。

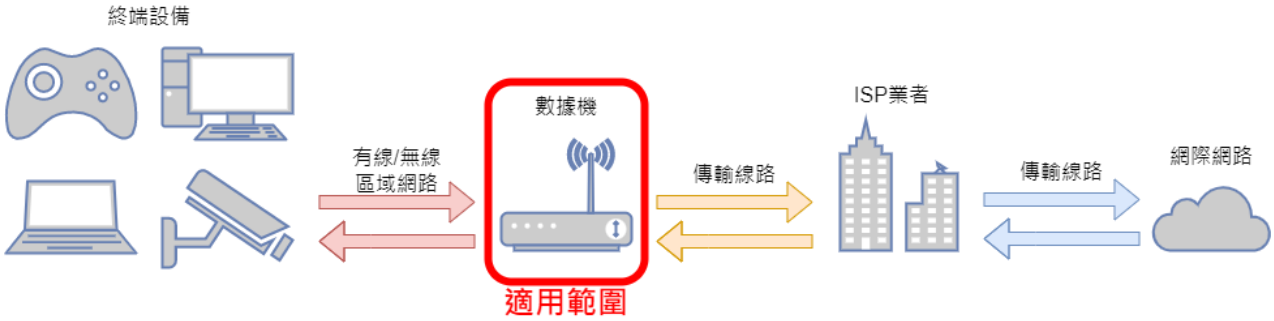

圖 1 適用範圍示意圖

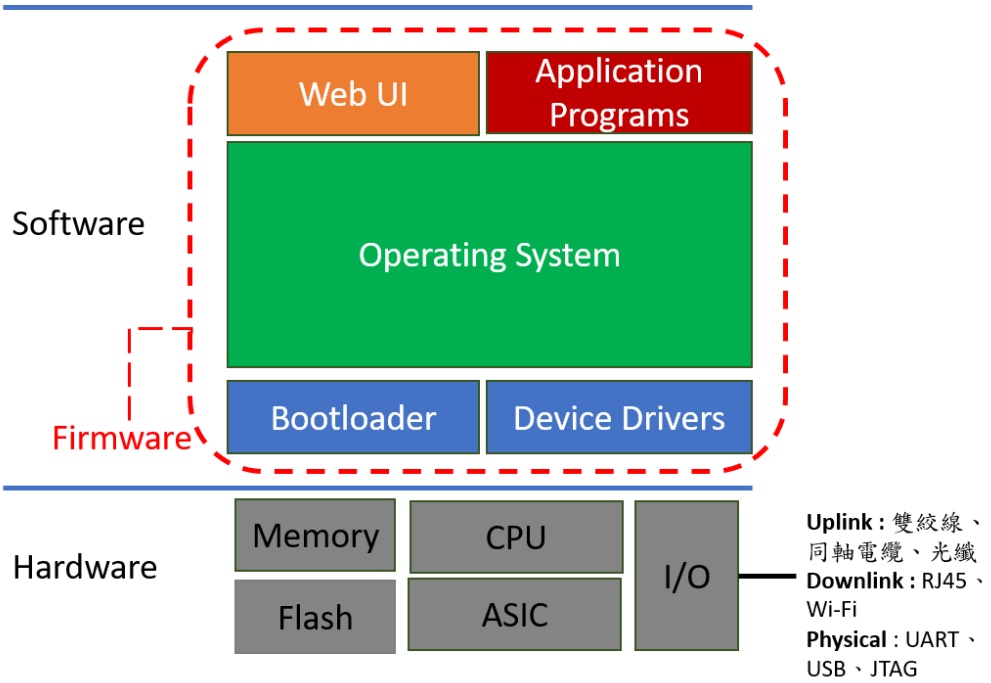

圖 2 數據機架構示意圖

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(含補充增修)。無加註年份者，適用其最新版(含補充增修)。

[1] IEC 62443-4-2:2019 (Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components)

[2] NIST SP 800-140C, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759

[3] NIST Special Publication 800-92, Guide to Computer Security Log Management

[4] TAICS TS-0045 v1.0 消費性物聯網產品資安標準

3. 用語及定義

下列用語與定義適用於本標準。

3.1 數據機

數據機為 Modulator（調變器）與 Demodulator（解調器）的簡稱，對通信設備所傳輸訊號進行調變或解調的設備，能將與資料處理設備相容的資料形式轉換為與傳輸設備相容的資料形式，或進行相反的解調轉換。

3.2 安全事件

安全事件泛指與系統操作以及系統異常之事件紀錄，包括管理介面及系統之登入、登出、修改通行碼及設定、異常狀況等。

3.3 日誌輪替(Log Rotate)

日誌輪替是指系統管理中一個自動化歸檔過期日誌文件的過程，其中包含日誌的分割與轉存，每當產生新的事件紀錄時，將會以其設計之時間、空間、存取位置及輪轉條件參數進行日誌文件管理，如日誌紀錄新增過程達到時間或空間參數條件時，將進行日誌分割，舊日誌文件名後面的數字即會增加，並依據存取位置進行儲存，若已滿足輪轉條件時，日誌可依據其設計方式進行刪除或者轉存到他處來釋放儲存空間以達成一次日誌輪替。日誌輪替提供了一個有效的方法來限制日誌文件的大小，同時保留近期的日誌用於分析。

3.4 國家弱點資料庫(National Vulnerabilities Database, NVD)

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的美國國家弱點資料庫，負責常見弱點與漏洞(如 3.5 所述)之資料的發布及更新。

3.5 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。

3.6 通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)

由資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST) 提供的漏洞評分系統，以衡量軟體漏洞的特徵和嚴重性進行評分。

3.7 管理者(Administrator)

具更改產品設定、作業系統、控制介面、功能應用程式之權限人員，如系統管理者。

3.8 加密(Encryption)

指為了避免資訊的洩漏，明文資訊透過數學演算法進行改變，使原來的明文資訊變成不可直接識別其原始之資訊，從而達到保密之目的。

3.9 安全通道(Security Tunnel)

為網際網路通訊端點與端點(End-to-End)間，並達到資料隱密性及完整性所建立之通道，如：目前常見之實作安全套接層協定 (Secure Sockets Layer, SSL)和傳輸層安全性協定(Transport Layer Security, TLS)。

3.10 敏感性資料(Sensitive Data)

指洩漏時可能對使用者造成損害之資料，不限但至少包含個人資料、通行碼、金鑰或地理位置等。此等資料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體建立、儲存或傳輸。

3.11 遠端連線(Remote Connection)

提供使用者可透過網路連線的方式，在網路另一端連接到提供服務的軟體或硬體設備。

3.12 身分鑑別(User Authentication)

一種電腦存取控制之方法，允許軟體與設備用以鑑別使用者身分之機制，並可防止未經授權之用戶存取敏感性資料之關鍵步驟。藉由通行碼、生物特徵、智慧卡...等身分鑑別機制可用以判別使用者是否為合法使用者。

3.13 通用平台枚舉(Common Platform Enumeration, CPE)

CPE 是資訊系統、軟體和軟體套件的結構化命名方式。基於統一資源標識符(URI) 的通用語法，CPE 包括正式名稱格式、用於根據系統檢查名稱的方法以及用於將文本和測試綁定到名稱的描述格式，並由美國國家弱點資料庫(NVD)平台提供已紀錄之 CPE 字典檔案及基本查詢服務。

3.14 軟體物料清單(Software Bill of Materials, SBOM)

軟體物料清單（SBOM）為軟體組件成分列表，透過提高軟體透明度，以進行軟體安全和軟體供應鏈風險管理。

3.15 通行碼

通行碼為密碼、暗號、通行字，是一種用於身分驗證的保密字符串，以達到保護隱私及防止未經授權的操作。

4. 安全等級

安全等級係為定義產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

本標準為數據機之共通安全要求，安全要求總表如表 1 所示，第一欄為安全構面，包括：(1)實體安全、(2)韌體安全及更新、(3)系統安全、(4)傳輸通訊安全、(5)身分鑑別機制安全、(6)網頁服務安全、(7)日誌紀錄安全；第二欄為安全要求分項，依各安全構面設計之對應安全要求項目；第三欄為安全等級，按各安全要求分項之驗證結果作為安全等級評估標準。本安全要求總表各欄位的關聯性，須依循章節 5 之技術規範內容。

安全等級依(1)相關資安風險高低、(2)資料保護程度，分為 1 級、2 級、3 級三個等級。1 級適用於供消費者使用之產品；2 級適用於企業或工廠使用之產品；3 級適用於政府單位或關鍵基礎設施使用之產品。產品須應先通過初階安全等級之測試，始可進行高階等級之測試。

表 1 安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
5.1 實體安全	5.1.1 實體埠安全管控	5.1.1.1*	-	-
5.2 韌體安全及更新	5.2.1 韌體更新	5.2.1.1*	5.2.1.2	-
	5.2.2 韌體更新檔之真確性與完整性	5.2.2.1*	-	-
	5.2.3 韌體傾印(dump)之敏感性資料	-	-	5.2.3.1
5.3 系統安全	5.3.1 作業系統與網路服務重大資安風險之漏洞	5.3.1.1	5.3.1.2	5.3.1.3
	5.3.2 最小化網路服務連接埠	5.3.2.1*	-	-
	5.3.3 敏感性資料之儲存加密	5.3.3.1*	-	-
	5.3.4 安全晶片之儲存保護聲明	-	-	5.3.4.1*
	5.3.5 遠端連線服務安全性	5.3.5.1*	-	-
5.4 傳輸通訊安全	5.4.1 網頁管理介面之傳輸安全	5.4.1.1*	-	-
	5.4.2 儲存媒體共用模式之傳輸安全	5.4.2.1	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
	5.4.3 Wi-Fi 傳輸安全	5.4.3.1*	-	-
	5.4.4 安全的 Wi-Fi 組態設置	5.4.4.1	-	-
	5.4.5 安全的數據機組態設置	5.4.5.1	-	5.4.5.2
5.5 身分鑑別機制安全	5.5.1 會話安全性	5.5.1.1	-	-
	5.5.2 檔案共享功能之權限控管機制	5.5.2.1	-	-
	5.5.3 預設通行碼安全性	5.5.3.1*	-	-
	5.5.4 通行碼鑑別機制強度	5.5.4.1	-	-
	5.5.5 通行碼的輸入頻率及次數限制	5.5.5.1*	-	-
5.6 網頁服務安全	5.6.1 管理者登入會話有效時間	5.6.1.1	-	-
	5.6.2 網頁管理介面重大資安風險之漏洞	5.6.2.1	5.6.2.2	5.6.2.3
	5.6.3 應用程式重送攻擊安全測試	-	-	5.6.3.1*
	5.6.4 設備設定檔內容之敏感性資料與權限管理	5.6.4.1*	-	-
5.7 日誌紀錄安全	5.7.1 安全事件日誌	5.7.1.1	5.7.1.2	-
	5.7.2 日誌內容之敏感性資料	5.7.2.1	-	-
	5.7.3 日誌輪替功能	5.7.3.1	5.7.3.2	5.7.3.3

註：以上項目編號後標示*字樣者，為參考 TAICS TS-0046 消費性物聯網產品資安測試規範。

4.1.1 安全構面

(a) 實體安全：產品測試用連接埠的處置，應視為實體安全要求之標的。

(b) 韌體安全及更新：產品之韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(c) 系統安全：產品之系統、網路服務應防止漏洞及具備即時檢視漏洞之安全機制，以及資訊安全管理的預防與處置機制。

(d) 傳輸通訊安全：產品敏感性資料之通訊安全，和通訊服務是否存在未知之資安漏洞，應視為傳輸通訊安全要求之標的。

(e) 身分鑑別機制安全：產品溝通介面須確保鑑別、授權及權限控管相關機制，包括遠端指令管理介面、通訊協定等，須具備一定防護能力，避免遭受蓄意人士入侵。

(f) 網頁服務安全：產品之網頁管理介面須具備足夠之安全防護機制。

(g) 日誌紀錄安全：產品之日誌紀錄應防止機敏資料之曝露。

4.1.2 安全要求分項

依安全構面所設計對應之安全要求要項，其中每一安全要求分項包含一個或一個以上之安全要求。

4.1.3 安全等級

安全等級依相關資安風險高低之綜合考量，分為 1 級、2 級、3 級三個等級。其對應之列即其所須符合之安全要求分項，安全等級級數的大小代表安全等級的高低，欲符合較高等級之安全要求必須先滿足較低安全等級要求。

5. 標準規範

本節詳盡載明數據機為滿足安全功能應採取的方法，數據機產品應依安全等級要求符合本節中安全基本要求。

5.1 實體安全

5.1.1 實體埠安全管控

5.1.1.1 實體埠之安全管控測試

產品之實體連接介面(例如：UART (Universal Asynchronous Receiver/Transmitter)、JTAG (Joint Test Action Group)、USB (Universal Serial Bus) 等)預設須關閉，或須經過身分鑑別方可存取作業系統之除錯模式，若為通行碼鑑別程序，則須符合 5.5.4 通行碼鑑別機制強度要求。

5.2 韌體安全及更新

5.2.1 韌體更新

5.2.1.1 韌體更新測試

產品須具備韌體更新機制，並提供韌體安全性更新方法。

5.2.1.2 韌體更新失敗復原測試

產品韌體更新失敗時，產品具備系統能回復更新前正常運作之能力。

5.2.2 韌體更新檔之真確性與完整性

5.2.2.1 韌體真確性與完整性測試

產品須具備確認置換之韌體真確性與完整性之能力。

5.2.3 韌體傾印(Dump)之敏感性資料

5.2.3.1 韌體傾印(Dump)之敏感性資料測試

產品韌體不應存在以明文顯示之敏感性資料，其加密方式須採用 NIST SP 800-140C 所核可之加密演算法，或晶片具有防讀取機制。

5.3 系統安全

5.3.1 作業系統與網路服務重大資安風險之漏洞

5.3.1.1 作業系統與網路服務重大資安風險之漏洞 1 級測試

產品作業系統與網路服務，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 9.0 以上(含 9.0)之共同資安弱點與漏洞。

5.3.1.2 作業系統與網路服務重大資安風險之漏洞 2 級測試

產品作業系統與網路服務，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 7.0 以上(含 7.0)之共同資安弱點與漏洞。

5.3.1.3 作業系統與網路服務重大資安風險之漏洞 3 級測試

產品作業系統與網路服務，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 4.0 以上(含 4.0)之共同資安弱點與漏洞，且須提供 SBOM 清單，其中不應存在 NIST NVD CPE 列表中可對應 CVSS 為 HIGH 以上(包含 HIGH)的基本風險計量評分。

5.3.2 最小化網路服務連接埠

5.3.2.1 最小化網路服務連接測試

產品非必要服務所需的網路埠須預設為關閉。

5.3.3 敏感性資料之儲存加密

5.3.3.1 敏感性資料之儲存加密測試

產品應加密儲存敏感性資料，其加密方式須採用 NIST SP 800-140C 所核可之加密演算法。

5.3.4 安全晶片之儲存保護聲明

5.3.4.1 安全晶片之儲存保護聲明

產品應使用安全晶片保護儲存之敏感性資料。

5.3.5 遠端連線服務安全性

5.3.5.1 遠端連線服務安全性測試

產品開啟遠端連線服務時，應於啟用時顯示警語，且遠端連線服務須通過身分鑑別後使用，若為通行碼鑑別程序，則須符合 5.5.4 通行碼鑑別機制強度要求。

5.4 傳輸通訊安全

5.4.1 網頁管理介面之傳輸安全

5.4.1.1 網頁管理介面之傳輸安全測試

產品網頁管理介面資料應透過安全通道傳輸，以確保資料之機密性、正確性及完整性，且安全通道版本須符合「傳輸層安全性協定 v1.2 同等或以上之安全通訊協定」的要求。

5.4.2 儲存媒體共用模式之傳輸安全

5.4.2.1 儲存媒體共用模式身分驗證測試

產品使用檔案共用服務應通過通行碼或其他依廠商宣告足以鑑別使用者身分之機制，若為通行碼鑑別程序，則須符合 5.5.4 通行碼鑑別機制強度要求。

5.4.3 Wi-Fi 傳輸安全

5.4.3.1 Wi-Fi 傳輸安全測試

產品應使用 WPA2 同等或以上之 Wi-Fi 安全通道。

5.4.4 安全的 Wi-Fi 組態設置

5.4.4.1 安全的 Wi-Fi 組態設置測試

產品須提供使用者得自行開/關「Wi-Fi 保護設置 (WPS)」之 「WPS PIN」及「WPS PBC」 功能，WPS 功能預設值皆須為關閉狀態。

5.4.5 安全的數據機組態設置

5.4.5.1 安全的數據機組態設置 1 級測試

產品須提供使用者得自行開/關 UPnP 功能，並於啟用時顯示警語。

5.4.5.2 安全的數據機組態設置 3 級測試

產品須滿足 5.4.5.1 之要求，且 UPnP 功能預設值須為關閉狀態。

5.5 身分鑑別機制安全

5.5.1 會話安全性

5.5.1.1 管理者會話安全性測試

產品僅允許單一管理者同時只有一個有效會話。

5.5.2 檔案共享功能之權限控管機制

5.5.2.1 檔案共享功能之權限控管機制測試

若產品有共享檔案的存取權限，須具備身分鑑別授權。

5.5.3 預設通行碼安全性

5.5.3.1 預設通行碼安全性之測試

不應使用共通的預設通行碼。

5.5.4 通行碼鑑別機制強度

5.5.4.1 通行碼鑑別機制強度測試

產品通行碼須符合政府組態基準(Government Configuration Baseline, GCB)、國際標準之強度要求或 TAICS TS-0050 v1.0 數據機資安測試規範 5.5.4.1 之判定標準要求。

5.5.5 通行碼的輸入頻率及次數限制

5.5.5.1 通行碼的輸入頻率及次數限制測試

產品在登入通行碼的設計上須有輸入頻率、次數及錯誤鎖定時間的限制，以防止遭受暴力破解。

5.6 網頁服務安全

5.6.1 管理者登入會話有效時間

5.6.1.1 管理者登入會話有效時間測試

管理者登入後，須存在閒置時限機制。

5.6.2 網頁管理介面重大資安風險之漏洞

5.6.2.1 網頁管理介面重大資安風險之漏洞 1 級測試

產品之之網頁管理介面，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 9.0 以上(含 9.0)之資安風險漏洞。

5.6.2.2 網頁管理介面重大資安風險之漏洞 2 級測試

產品之之網頁管理介面，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 7.0 以上(含 7.0)之資安風險漏洞。

5.6.2.3 網頁管理介面重大資安風險之漏洞 3 級測試

產品之之網頁管理介面，不應存在通用漏洞評分系統 CVSS 基本風險計量評分為 4.0 以上(含 4.0)之資安風險漏洞。

5.6.3 應用程式重送攻擊安全測試

5.6.3.1 應用程式重送攻擊安全測試

產品之網頁服務與應用程式介面須具備身分鑑別機制與防止重送攻擊，如透過通行碼鑑別程序，則須符合 5.5.4 通行碼鑑別機制強度要求。

5.6.4 設備設定檔內容之敏感性資料與權限管理

5.6.4.1 設備設定檔內容之敏感性資料與權限管理測試

產品設備設定檔之匯入與匯出功能須具有管理權限要求，並且其輸出之內容不應存在明文顯示之敏感性資料，應用加密方式來儲存敏感性資料，其加密方式須採用 NIST SP 800-140C 所核可之加密演算法。

5.7 日誌紀錄安全

5.7.1 安全事件日誌

5.7.1.1 安全事件日誌 1 級測試

產品須具備管理介面及系統之登入、登出、修改通行碼、設定及異常狀況之安全事件紀錄，並確實記錄年月日、時分秒之事件時間及事件內容。

5.7.1.2 安全事件日誌 2 級測試

產品須符合 5.7.1.1 之要求，且須具備將日誌記錄至外部儲存空間或 Log 伺服器之功能。

5.7.2 日誌內容之敏感性資料

5.7.2.1 日誌內容之敏感性資料測試

產品日誌紀錄中不應存在敏感性資料。

5.7.3 日誌輪替功能

5.7.3.1 日誌輪替功能 1 級測試

產品之事件日誌須具備日誌輪替機制，且應根據 NIST SP 800-92 Table 4-1「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Low

Impact Systems 類別，產品設備應提供足夠容納該範例最低日誌保留天數總計所需以上的日誌儲存容量。

5.7.3.2 日誌輪替功能 2 級測試

產品之事件日誌須具備日誌輪替機制，且應根據 NIST SP 800-92 Table 4-1「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 Moderate Impact Systems 類別，產品設備應提供足夠容納該範例最低日誌保留天數總計所需以上的日誌儲存容量。

5.7.3.3 日誌輪替功能 3 級測試

產品之事件日誌須具備日誌輪替機制，且應根據 NIST SP 800-92 Table 4-1「Examples of Logging Configuration Settings」所呈現的日誌組態設定範例之 High Impact Systems 類別，產品設備應提供足夠容納該範例最低日誌保留天數總計所需以上的日誌儲存容量。

附錄 A
(規定)
安全通道版本使用要求

係指超文本傳輸協定(HTTP)結合安全套接層協定(SSL)或傳輸層安全性協定(TLS)，建立安全通道以保護傳輸中資料不被竊取之技術，然而 SSL 在 2014 年 10 月由 Google 指出其資訊安全漏洞，宣布全面禁用，所以已經完全由 TLS 取代。但 TLS 1.0 存在可以降級到 SSL 3.0 的功能，使得 TLS 1.0 同樣不被信任，因此目前本標準應使用的版本為：TLS v1.2 以上之版本。

附錄 B
(參考)
安全要求與國際標準對照

表 B.1 安全要求與國際標準對照表

安全構面	安全要求	對應項目	參考來源	參考內容
實體安全	實體埠安全管控測試	本標準 5.1.1	OWASP IoT Top Ten 2018	10：Lack of Physical Hardening
韌體安全及更新	韌體更新測試	本標準 5.2.1	OWASP IoT Top Ten 2018	4：Lack of Secure Update Mechanism
			IEC 62443-4-2	FR 3 - System integrity
	韌體更新檔之真確性及完整性測試	本標準 5.2.2	OWASP IoT Top Ten 2018	4：Lack of Secure Update Mechanism
			IEC 62443-4-2	FR 3 - System integrity
	韌體傾印(Dump)之敏感性資料測試	本標準 5.2.3	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
系統安全	作業系統與網路服務重大資安風險之漏洞測試	本標準 5.3.1	OWASP IoT Top Ten 2018	2：Insecure Network Services 5：Use of Insecure or Outdated Components
			IEC 62443-4-2	FR 3 - System integrity
	最小化網路服務連接埠測試	本標準 5.3.2	OWASP IoT Top Ten 2018	2：Insecure Network Services
			IEC 62443-4-2	FR 7 - Resource availability
	敏感性資料之儲存加密測試	本標準 5.3.3	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data

安全構面	安全要求	對應項目	參考來源	參考內容
				confidentiality
	安全晶片之儲存保護聲明測試	本標準 5.3.4	IEC 62443-4-2	FR 1 - Identification and authentication control
	遠端連線服務安全性測試	本標準 5.3.5	OWASP IoT Top Ten 2018	2：Insecure Network Services
			IEC 62443-4-2	FR 1 - Identification and authentication control
傳輸通訊安全	網頁管理介面之傳輸安全測試	本標準 5.4.1	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 3 - System integrity
	儲存媒體共用模式之傳輸安全測試	本標準 5.4.2	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 3 - System integrity
	Wi-Fi 傳輸安全測試	本標準 5.4.3	OWASP IoT Top Ten 2018	9：Insecure Default Settings
			IEC 62443-4-2	FR 3 - System integrity
	安全的 Wi-Fi 組態設置測試	本標準 5.4.4	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces 9：Insecure Default Settings
			IEC 62443-4-2	FR 2 - Use control
	安全的數據機組態設置測試	本標準 5.4.5	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces 9：Insecure Default Settings
			IEC 62443-4-2	FR 2 - Use control
身分辨識	會話安全性測試	本標準 5.5.1	OWASP IoT Top Ten 2018	9：Insecure Default Settings

安全構面	安全要求	對應項目	參考來源	參考內容
安全機制			IEC 62443-4-2	FR 1 - Identification and authentication control
	檔案共享功能之權限控管機制測試	本標準 5.5.2	IEC 62443-4-2	FR 2 - Use control
	預設通行碼安全性測試	本標準 5.5.3	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 1 - Identification and authentication control
	通行碼鑑別機制強度測試	本標準 5.5.4	OWASP IoT Top Ten 2018	1：Weak, Guessable, or Hardcoded Passwords
			IEC 62443-4-2	FR 1 - Identification and authentication control
	通行碼的輸入頻率及次數限制測試	本標準 5.5.5	OWASP IoT Top Ten 2018	9：Insecure Default Settings
			IEC 62443-4-2	FR 1 - Identification and authentication control
網頁服務安全	管理者登入會話有效時間測試	本標準 5.6.1	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
	網頁管理介面重大資安風險之漏洞測試	本標準 5.6.2	OWASP IoT Top Ten 2018	5：Use of Insecure or Outdated Components
			IEC 62443-4-2	FR 3 - System integrity
	應用程式重送攻擊安全測試	本標準 5.6.3	OWASP IoT Top Ten 2018	3：Insecure Ecosystem Interfaces
			IEC 62443-4-2	FR 3 - System integrity
	設備設定檔內容之敏感性資料與權限管理測試	本標準 5.6.4	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data

安全構面	安全要求	對應項目	參考來源	參考內容
				confidentiality
日誌紀錄安全	安全事件日誌測試	本標準 5.7.1	IEC 62443-4-2	FR 2 - Use control
	日誌內容之敏感性資料測試	本標準 5.7.2	OWASP IoT Top Ten 2018	7：Insecure Data Transfer and Storage
			IEC 62443-4-2	FR 4 - Data confidentiality
	日誌輪替功能測試	本標準 5.7.3	IEC 62443-4-2	FR 2 - Use control
			NIST SP 800-92	Table 4-1. Examples of Logging Configuration Settings

附錄 C
(參考)
風險來源分析與資安需求

表 C.1 風險來源分析與資安需求表

1. Spoofing（非法冒用）

ID	Threat	Vulnerability	Undesirable Consequence
S-01	惡意活動/濫用 Nefarious activity / Abuse	遭惡意裝置偽造 Counterfeit by malicious devices	這種威脅很難發現，因為假冒設備無法輕易地與原設備作區分。 而這些偽造的設備通常具有後門，可對於該網路環境中的其他 ICT 系統進行攻擊。
S-02	竊聽/攔截/劫持 Eavesdropping/ Interception/ Hijacking	中間人攻擊 Man in the middle	在兩端使用者在訊息傳輸間進行竊聽攻擊，攻擊者從中攔截訊息竄改後再轉送，以使兩端使用者相信正在與彼此直接通話。
S-03		會話挾持 Session hijacking	透過介入 admin 登入數據機管理介面（Web UI）之間，劫持會話得以執行中間人攻擊，冒充該合法設備。(MITM)
S-04		重送訊息 Replay of messages	此攻擊透過惡意地重複發送有效資料傳輸或延遲資料傳輸，來執到操縱或癱瘓（crash）目標設備。
S-05	損壞/損失 Damage/ Loss	憑證保護不足 Weak Credential Storage	金鑰儲存未加密或權限控管不當，當被輕易破解入侵，恐遭受更嚴重的攻擊。

2. Tampering（竄改）

ID	Threat	Vulnerability	Undesirable Consequence
T-01	惡意活動/濫用 Nefarious activity / Abuse	惡意程式 malware	在未經用戶同意的情況下對系統執行不必要和未經授權的操作的軟體程序，從而導致損壞，破壞或信息盜用。 它的影響可能很大。
T-02		遭惡意裝置偽造 Counterfeit by malicious devices	重刷有帶惡意程式的韌體，或從實體/遠端通訊介面入侵更新韌體，取得管理者權限，可以控制該合法機器，執行任意動作。
T-03	失效/故障 Failures / Malfunctions	第三方失效 Third parties failures	一個作動中的元件發生錯誤的原因，可能是由於另一元件設定錯誤而引起的。例如，DHCP 設定被開啟、wifi 安全協定設定選用 WEB 或遠端設定等。
T-04	實體攻擊 Physical attacks	設備修改 Device	利用設備 port 不良的設定來達到竄改設備，例如：竄改系統組態檔、管理介面

ID	Threat	Vulnerability	Undesirable Consequence
		modification	帳密，以達控制該合法設備目的。

3. Repudiation（否認）

ID	Threat	Vulnerability	Undesirable Consequence
R-01	惡意活動/濫用 Nefarious activity / Abuse	審察不足 Insufficient Auditing	安全事件紀錄記載的資訊如不能足以對發生的情況說明清楚，當發生抵賴（repudiation）安全事件時，則無法證明是否有非法登入、竄改等情事。包括，使用者、時間、事件摘要、數據來源等。
R-02		可更新紀錄檔的事件紀錄可信度低 Lower Trusted Subject Updates Logs	安全事件紀錄如不具備權限控管，則任何使用者皆能查看、修改或刪除，將造成發生安全事件時無法追朔或證明。

4. Information disclosure（資訊披露）

ID	Threat	Vulnerability	Undesirable Consequence
I-01	惡意活動/濫用 Nefarious activity / Abuse	針對性的攻擊 Targeted attacks	潛藏監聽很長一段時間，利用時機分且分多個階段對特定目標發動的攻擊。 主要目的是保持隱藏竊聽並獲取敏感資料/訊息或控制指令。 （威脅的影響中等，但通常很難檢測到它們並且需要很長時間）
I-02	竊聽/攔截/劫持 Eavesdropping/ Interception/ Hijacking	通訊協議劫持攻擊 protocol hijacking	控制網路兩端（elements）之間的通信對話（communication session）。挾持的方法可以使用像強制斷線或拒絕服務（denial of service）之類的攻擊技術。 例如：利用通訊協議的漏洞，入侵者能夠嗅探到包括通行碼在內的敏感資訊。 當設備（ex. router）被有意或無意的將設定設置錯誤（ex.路由表），遭受到 BGP hijacking 攻擊，造成流量過大以致癱瘓網路。
I-03		截取訊息 Interception of information	未經授權的攔截（有時是修改）私人通訊，例如電話、即時訊息、電子郵件通訊等。
I-04		資料流嗅探 Data Flow Sniffing	攻擊者可能會嗅探跨 HTTP 傳輸的數據。根據攻擊者可以讀取什麼類型的資料，它可能會被用於攻擊系統的其他部分，或者僅僅是導致違反合規性的信息披露。考慮加密資料流。
I-05		網路探查 Network reconnaissance	被動獲取網路內部訊息：連接的設備、使用的通訊協定、開啟的 ports、正在使用的服務等。
I-06	損壞/損失	資料/敏感資訊洩	將敏感資料有意或無意地洩漏給未被授權

ID	Threat	Vulnerability	Undesirable Consequence
	Damage / Loss	漏 Data / Sensitive information leakage	的使用者。此威脅重要性取決於洩漏的資料類型。 例如，設備存在不必要功能/服務，導致機密資料外洩，例:偷傳資料回惡意伺服器。
I-07		憑證保護不足 Weak Credential Storage	伺服器保存的憑證經常被洩露或篡改，且客戶端上儲存的憑證也經常被盜。對於服務器端，請考慮儲存憑證的雜湊演算法，而不是儲存憑證本身。 如果由於業務需求而無法做到這一點，請確保在儲存之前使用 SDL 批准的機制對憑證進行加密。 對於客戶端，如果需要儲存憑證，請對其進行加密並保護儲存憑證的資料儲存。
I-08		認證因子洩漏 Authentication factor leakage	當設備與 ISP（Internet Service Provider）進行 MAC 身分驗證時，或是 ISP 對電腦（網卡）進行身分驗證時，如果傳輸通道未加密而被有心人取得。
I-09	失效/故障 Failures / Malfunctions	繞過授權 Authorization Bypass	可以存取設備並繞過 admin 的設備/設備的權限。例如，通過直接使用十六進位編譯器編輯文件，或是通過文件共享來存取文件。

5. Denial of service（拒絕服務）

ID	Threat	Vulnerability	Undesirable Consequence
D-01	惡意活動/濫用 Nefarious activity / Abuse	DDoS	多個系統攻擊單個目標，以使其達到飽和並使其崩潰。 這可以通過建立許多連線讓一個連線通道塞爆，或一遍遍地重放相同的訊息來完成。
D-02		數據機或設備的潛在過量資源消耗 Potential Excessive Resource Consumption for Modem or Admin's Device	數據機或 admin 的設備/設備沒有採取明確的步驟來控制資源消耗。資源消耗攻擊可能很難處理，而且有時讓操作系統執行任務是有意義的。須注意您的資源請求不會 deadlock，但會超時。
D-03		阻斷服務 Denial of service	若數據機無日誌輪替功能，則事件紀錄檔案填滿設備儲存裝置時，將造成服務中斷或影響到設備運行。
D-04	執行中斷 Outages	失去支援服務 Loss of support services	系統正常運行所需的支援服務無法使用。

ID	Threat	Vulnerability	Undesirable Consequence
D-05	失效/故障 Failures / Malfunctions	軟體漏洞 Software vulnerabilities	常見 IoT 設備通常會因弱通行碼/默認通行碼、軟體 bugs 和設定錯誤而容易攻擊，對網路造成風險。

6. Elevation of privilege（提升權限）

ID	Threat	Vulnerability	Undesirable Consequence
E-01	惡意活動/濫用 Nefarious activity / Abuse	遭惡意裝置偽造 Counterfeit by malicious devices	利用遠端通訊介面入侵，(elevation of privilege 提升特權）取得管理權限以控制該設備。
E-02	實體攻擊 Physical attacks	通過更改數據機中的執行程序來提升權限 Elevation by Changing the Execution Flow in Modem	攻擊者可能會將資料（數據）傳遞到數據機中，來將數據機中的程序執行流程改為攻擊者決定。透過提權後，竄改 modem 參數。例如，數據機管理介面（Web UI）對外部呼叫流量檢查不完全造成的驗證繞過（authentication bypass）漏洞。駭客可經由 HTTP 或 HTTPS 傳送惡意呼叫開採本漏洞，使未獲授權的遠端攻擊者得以上傳任意檔案、修改產品設定，或注入反向 Shell 指令。
E-03		使用遠程執行代碼，modem 可能會提升特權 Modem May be Subject to Elevation of Privilege Using Remote Code Execution	admin 的設備或其他設備可能能夠遠端執行 modem 的指令。 例如，設備 Web UI 對使用輸入指令驗證不足，及程式未做好邊界檢查（boundary checks），使未授權的遠端使用者進行緩衝區溢位攻擊，取得作業系統根權限。
E-04		提升特權 elevation of privilege	利用實體介面入侵，(elevation of privilege 提升特權）取得管理權限以控控該設備。

參考資料

(1) FIPS 140-2 Annex A: National Institute of Standards and Technology (NIST),Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Module, May 10, 2017.
(2) Cybersecurity Framework, Version 1.1. 2018/04/16
(3) U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT), Version 1.0, 2016-11-15
(4) SB-327 Information privacy: connected devices. 2017
(5) European Commission Cybersecurity Act. 2017/11/19
(6) European Parliament, The Directive on security of network and information systems (NIS Directive), EUR-Lex - 32016L1148 - EN, 2016/7/6
(7) European Parliament, Regulation on Privacy and Electronic Communications, EUR-Lex - 52017PC0010 – EN
(8) International Organization for Standardization, Are we safe in the Internet of Things? https://www.iso.org/news/2016/09/Ref2113.html
(9) ISO/IEC 27030 (Information technology - Security techniques - Guidelines for security and privacy in Internet of Things (IoT))
(10) ISO/IEC 15408-1: 2009 (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.)
(11) International Electro technical Commission, About IEC https://www.iec.ch/about/
(12) IEC 62443-4-1:2018 (Security for industrial automation and control systems –Part 4-1: Secure product development lifecycle requirements)
(13) SAE-J 3061:2016 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)
(14) IEEE Standard Association, P2413.1 (Standard for a Reference Architecture for Smart City (RASC))
(15) ENISA, Baseline Security Recommendations for IoT. 2017/11/20
(16) ENISA, Good Practices for Security of Internet of Things in the context of Smart Manufacturing, 2018/11/19
(17) UL 2900-1 (Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements), 2017/7/5

(18) UL2900-2-2 (Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems), 2016/3/30
(19) ETSI, Cyber Security for Consumer Internet of Things, TS 103 645, Version 1.1.1, 2019/2/19
(20) https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
(21) NIST SP 800-92 Guide to Computer Security Log Management Table 4-1
(22) https://nvd.nist.gov/products/cpe

版本修改紀錄

版本	時間	摘要
v1.0	2022/09/15	出版

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw