醫療器材網路安全評估分析參考範本

「血氧濃度應用軟體」

衛生福利部食品藥物管理署

111 年 3 月

本範本不具法規強制性，僅提供業者建議或參考使用。

引言

本醫療器材網路安全評估分析參考範本係以衛生福利部食品藥物管理署公告之「適用於製造業者之醫療器材網路安全指引」為基礎，協助業者制定醫療器材網路安全評估報告。

本範本不具法規強制性，僅提供業者建議或參考使用。醫療器材業者如有既定網路安全評估格式，只要能涵蓋本署「適用於製造業者之醫療器材網路安全指引」範圍皆可適用。另範本所列各式文字僅供參考，醫療器材業者仍需視產品本身特性及實際操作流程擬訂，並以其為基礎執行網路安全評估。

ABC醫材股份有限公司

醫療器材網路安全評估報告
Cybersecurity Risk Assessment Report for Medical Device

血氧濃度應用軟體

報告基本資訊(Basic Information of the Report)

報告編號 (Report No.)	ABCSWAPP	報告版本 (Report Version)	V1.0
公司名稱 (Company Name)	ABC醫材股份有限公司		
電話(TEL)	02-XXXX-XXXX	傳真(FAX)	02-XXXX-XXXX
製造業者地址 (Factory Address)	OO市XX區XX路X號X樓		
審查者 (Review By)	報告製作者 (Prepared By)	評估日期 (Evaluation Period)	報告日期 (Report Date)
YZ	Eric Leo	111/03	111/03

中華民國 111年 3月

目 錄

1. 簡介(Introduction)

1.1 報告概述(Document Overview)

本報告包括醫療器材「血氧濃度應用軟體」之醫療器材組成元件、軟體物料清單、軟體設計暨發展、網路安全風險評鑑報告、網路安全自我檢核與檢測報告等。(This document covers the security risk assessment report of Product name device, designed in Product name software development project.)因此，本報告包括：

- 風險分析 The risk analysis,
- 風險評鑑報告 The risk assessment report,
- 風險追蹤矩陣 The risk traceability matrix with software requirements.

1.2 評估團隊(Evaluation Team)

姓名 Name	部門 Dept.,	職稱 Title	學歷 Education	經歷 Experience	專長 Specialty	工作年資 Seniority	責任 Responsibility
趙 OO	R&D	協理	XX 大學資工系 博士	OO 公司 研發工程師	ICCP 認證	15 年	產品安全評估、產品整合評估與測試
張 OO	R&D	工程師	XX 大學資工系 碩士	OO 公司 雲端研發工程師	機器學習 雲端系統設計	12	軟體開發及測試
呂 OO	R&D	工程師	XX 大學資工系 碩士	OO 電腦 網路管理工程師	生物訊號分析 演算法設計	10	軟體開發及測試
高 OO	品質管理部	副理	XX 大學電機系 碩士	OO 公司 品質管理工程師	OO 認證	9 年	品質管理
黃 OO	品質管理部	副理	XX 大學電機系 碩士	OO 生技 法規助理	OO 證照	9 年	品質管理

1.3 引用文件(Document References)

1.3.1 引用的專案文件(Project References)

序號 #	文件編號 Document Identifier	文件標題 Document Title
1	ABCSWAPP-123-01	Software Requirements Specification
2	ABCSWAPP-456-01	Software Architecture Design
3	ABCSWAPP-789-01	Software Validation Report
4	ABCSWFW-123-01	Firmware Requirements Specification
5	ABCSWFW-456-01	Firmware Architecture Design
6	ABCSWFW-789-01	Firmware Validation Report

1.3.2 引用的標準與法規(Standard and Regulatory References)

序號 # Document Identifier	文件編號 Document Identifier	文件標題 Document Title
1	ISO 14971:2019	Medical devices -- Application of risk management to medical devices
2	IEC 62304:2015	Medical device software - Software life cycle processes
3	AAMI TIR 57:2016	Principles for medical device security—Risk management
4	IEC 80001-2-8:2016	Application of risk management for IT-networks incorporating medical devices
5	NIST SP 800	Address and support the security and privacy needs of U.S. Federal Government information and information systems.

1.3.3 網路安全評估結果摘要(Summary of Cybersecurity Assessment Results)

ABC血氧濃度應用軟體於產品設計階段時已考量網路安全相關的問題，除了透過手機上原有的基礎保護外，同時對於APP與手機間的資料傳輸、資料存取進行加密，避免資料被竊取或竄改。

在網路安全風險評估方面，除了先由本團隊中的軟體安全評估人員先行驗證軟體安全，也將產品送至第三方軟體安全實驗室測試產品相關漏洞，並評估剩餘網路安全風險皆已為可接受的範圍內。此外產品於上市後也制定相關的檢查機制，幫助所有產品於發現網路安全漏洞時立即修復錯誤並更新軟體，避免對使用者造成風險。

2. 一般要求(General Requirement)

2.1 產品簡介(Product Introduction)

2.1.1 簡介與發展程序(Development Process)

ABC公司已實施合理的管理、技術和實質保護措施，防止ABC公司產品的安全事件和隱私洩露，前提是產品是按照ABC公司的使用說明所操作。然而，隨著系統和威脅的發展，沒有任何系統可以保護所有漏洞。我們認為我們的客戶是維護安全和隱私保護的最重要合作夥伴，在適當的情況下，我們將通過產品變更、技術公告或是披露相關資訊給客戶和監管機構。 ABC公司透過以下措施不斷努力提高整個產品生命週期內的安全性和隱私性：

- 隱私和安全設計
- 產品和供應商風險評估
- 漏洞和更新管理
- 安全編碼原則和分析
- 漏洞掃描和測試
- 適用於客戶數據的存取控制
- 事件應變
- 確保雙向通訊暢通無阻

本文檔的目的是詳細說明**ABC公司**安全和隱私範例如何應用於**本產品**，及您應該如何維護該產品安全的知識，以及我們如何與您合作，以確保該產品整個生命週期的安全。

2.1.2 預期用途(Intended Use)

為一使用在ABC智慧手錶上進行血氧的量測、紀錄、儲存以及顯示血氧資訊的軟體產品。ABC血氧濃度應用軟體會透過光體積變化描記圖法(PPG)此種無創檢測方法，用以檢測血管的收縮與擴張。透過演算法計算後轉換成血氧濃度比例之數值。於使用者休息狀態量測。此ABC血氧濃度應用軟體呈現的血氧資訊可做為**醫療保健**等等之檢測的參考依據，但在未諮詢過符合資格的醫療保健專業人員建議或是未經過標準的量測方法前，不適合以此ABC血氧濃度應用軟體呈現的血氧資訊來進行後續臨床診斷或治療。

2.1.3 軟硬體系統運作架構與軟體物料清單(System Operating Architecture And Software Bill Of Materials)

本產品系統架構如下：

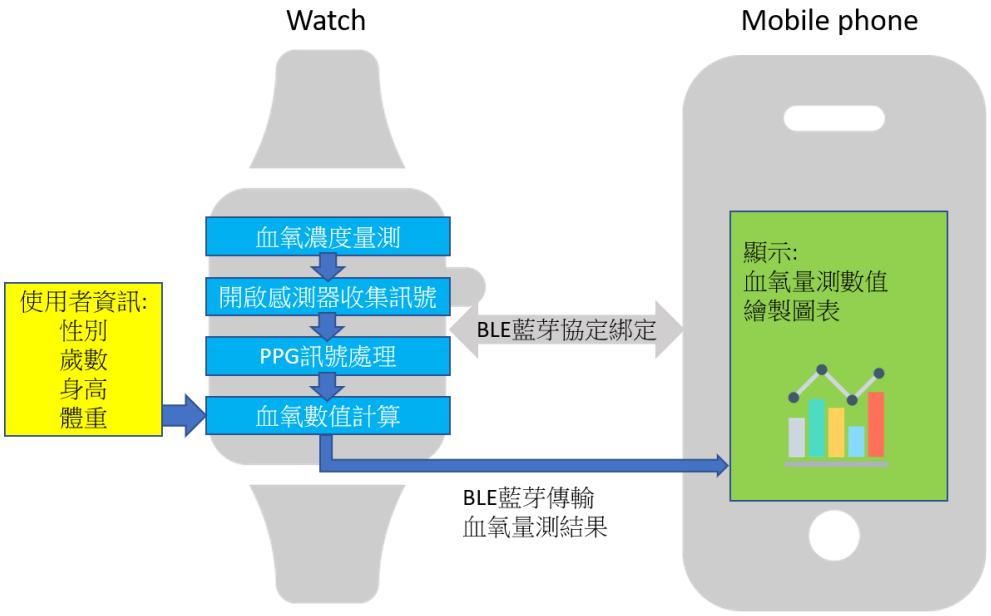


圖2.1.3.1、系統架構圖

ABC血氧濃度應用軟體系統包含手錶端的ABC智慧手錶與其中的ABC BO軟體以及手機端的ABC健康應用程式。使用者可透過手錶端進行之功能包含血氧濃度量測、檢視血氧數值，並將血氧濃度量測結果透過藍芽(Bluetooth Specification v4.0)傳出到手機端的ABC健康應用程式。使用者可透過手機端進行之功能為檢視血氧量測記錄與圖表之檢視。

本ABC血氧濃度應用軟體系統之主要應用情境為資料量測、資料檢視以及資料傳輸，如下表2.1.3.1。

表2.1.3.1、ABC血氧濃度應用軟體系統應用情境

應用情境	說明	資產
資料量測	使用者透過啟動手錶上的LED燈以及PPG感測器，量測血氧濃度	去識別化之個人資料:性別、年齡、身高、體重
資料檢視	使用者檢視其手錶或手機上之血氧資料	血氧濃度數值
資料傳輸	使用者透過與藍芽綁定之設備進行血氧濃度數值資料傳輸	通訊協定、血氧濃度數值資料

本ABC血氧濃度應用軟體系統運作時所需組成元素(資產)，如表2.1.3.2。

表2.1.3.2、ABC血氧濃度應用軟體系統資產清單

資產名稱	說明
血氧量測演算法	接收PPG訊號，經訊後處理演算法可推估出血氧濃度數值
血氧資料	血氧濃度，血液中血紅蛋白相對

	於總血紅蛋白（不飽和+飽和）的比例
通訊協定	BLE 4.0
個人資料	去識別化之性別、年齡、身高、體重等資料

ABC公司對於個人資料之蒐集、處理和利用皆符合我國《個人資料保護法》要求。因本產品涉及個人資料之蒐集、處理及利用，應遵守個人資料保護法之規範。

系統要求

類別	要求
ABC健康應用程式所支援的作業系統	Android 5.0+ iOS 10+
行動裝置螢幕解析度	320（建議的行動裝置最小像素寬度）

ABC血氧濃度應用軟體之軟體物料清單，如下表2.1.3.3。

表2.1.3.3、ABC血氧濃度應用軟體之軟體物料清單

名稱	來源	版本
Eclipse with C++	https://www.eclipse.org/downloads/	Eclipse IDE 2021-09
Docker	https://docs.docker.com/engine/release-notes/18.03/	18.03.1-ce
Python	https://www.python.org/downloads/release/python-370/	3.7.0
Xcode	https://developer.apple.com/xcode/	Xcode 13
Android Studio	https://developer.android.com/studio	2020.3.1 for Windows 64-bit

本產品中的資料皆受到密碼、加密以及系統內安全連接的保護。

- 密碼–所有帳戶都會使用強化密碼。密碼建立規則用於確保使用者建立的密碼不會輕易讓他人猜中。使用者需要保護好密碼，為保密資料的安全盡其應盡的責任。切勿向任何他人透露您的密碼。本公司絕不會向您索要密碼。
- 加密–儲存和傳輸資料時採用了加密來保護個人資訊，使預定使用者之外的任何人均無法讀取資料。
- 安全連接–僅透過與受信任的系統進行安全連接與資料傳輸，在此系統為透過藍芽BLE4.0 綁定之行動裝置。

2.2 網路安全要求(Security Requirement Specification, SRS)

本產品之網路安全要求乃參照衛生福利部食品藥物管理署「適用於製造業者之醫療器材網路安全指引」[1]及行政院國家資通安全會報技術服務中心[2]所規範之資通安全需求如下表2.2.1：

表2.2.1、網路安全要求檢核表

分類	問題	答案(是/否/不適用)	SRS
機密性	機敏資料傳輸時，採用加密機制	是	SRS-01
	機敏資料儲存時，採用加密機制	是	SRS-02
	使用公開、國際機構驗證且未遭破解的演算法	不適用	
	使用該演算法支援的最大金鑰長度	不適用	
	不使用自行創造的加密方式	是	SRS-03
	加密金鑰具有保護機制	不適用	
	加密金鑰或憑證週期性更換	不適用	
完整性	重要資料產生HASH值，確保其完整性	是	SRS-04
	重要資料傳輸過程，使用防止竄改的協定	是	SRS-05
	提供下載的資料，產生HASH值供比對其完整性	不適用	
可用性	評估服務重要性，設定可用性要求	不適用	
	採用「高可用性」(High Availability) 架構或機制	不適用	
	重要資料定時同步至備援環境	不適用	
輸入驗證	採用過濾機制，以防止輸入惡意命令或資料	是	SRS-06
	驗證使用者輸入資料	是	SRS-07
	驗證外部取得的資料	不適用	
	驗證系統參數合理性	是	SRS-08
	於伺服器端檢查輸入資料合法性	不適用	
身分認證	除了允許匿名存取的功能外，所有功能都必須經過認證才允許存取	不適用	
	身分認證機制位於伺服端且採用集中管理機制	不適用	
	採用多重因素認證(兩種以上認證類型)	不適用	
	採用CAPTCHA 機制於身分認證或重要交易行為，以防範自動化程式之嘗試	不適用	
	身分認證相關資訊不以明文傳輸	不適用	

[1] 衛生福利部食品藥物管理署. (2021). 適用於製造業者之醫療器材網路安全指引. Available: https://www.fda.gov.tw/TC/newsContent.aspx?cid=3&id=27018

[2] 行政院國家資通安全會報技術服務中心. 系統安全發展流程實務.

	身分認證相關資訊不存於源碼中，並限制存取	不適用	
	身分認證失敗達一定次數後鎖定該帳號	不適用	
	身分認證發生錯誤時，預設不允許存取任何功能	是	SRS-09
	密碼添加亂數資料(Salt)後進行雜湊函數(HASH)處理，才加以儲存	不適用	
	密碼須符合複雜度(長度限制、具備英文大小寫及特殊字元等)	不適用	
	限制需定期更換密碼	不適用	
	重要交易行為要求再次身分認證	不適用	
授權與存取控制	採用伺服端的集中管理機制檢查使用者授權	不適用	
	執行功能或存取資源前，檢查使用者授權	是	SRS-10
	除特殊管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)	不適用	
	使用者/角色賦予所需的最小權限	是	SRS-11
	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行	是	SRS-12
	重要行為由多人/角色授權後才得以進行	不適用	
日誌紀錄	認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行 Log 記錄	是	SRS-13
	Log 紀錄考慮包含以下項目 1.識別使用者之ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型(例如，成功或失敗)。5.事件優先權(priority)。6. 事件詳細描述。7.事件代碼。8.網路位址	不適用	
	採用單一的Log 機制，確保輸出格式的一致性	不適用	
	Log 進行適當保護及備份，避免未經授權存取	不適用	
會話管理	會話識別碼(Session ID)是隨機產生且不可預測	不適用	
	使用者的會話階段，設定在合理的時間內失效	不適用	
	使用者的會話階段，使用者登出後失效	不適用	
	使用者重新登入後，會話識別碼(Session ID)會改變	不適用	
	不將會話識別碼(Session ID)或使用者 ID 顯示於使用者可以改寫處	不適用	
錯誤及例外管理	所有的功能都會進行錯誤及例外處理，並將資源正確釋放	是	SRS-14
	軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息	不適用	
	嚴重錯誤採用通知機制(例如電子郵件或簡訊)	不適用	
組態管理	管理者介面限制存取來源或不允許遠端存取	不適用	

	參數設定或系統設定存放處，限制存取或進行適當保護	不適用	
	依賴的外部元件或軟體，不使用預設帳號密碼	是	SRS-15
	作業平台定期更新、關閉不必要服務、注意安全設定	是	SRS-16
	依賴的外部元件或軟體，注意其安全漏洞通告，必要時進行評估並更新	是	SRS-17

本產品根據上述資通安全規範自主檢查表，確認網路安全要求如下表2.2.2：

表2.2.2、適用項目需求分析

SRS編號 No(SRS)	網路安全要求規格說明(Security Requirement Specification SRS Description)
SRS-01	血氧量測資料傳送時需採用加密通訊協定
SRS-02	血氧量測資料接收端儲存資料時會做加密處理
SRS-03	血氧量測資料傳送、儲存時，不使用自行創造的加密方式
SRS-04	血氧量測資料會使用雜湊(HASH)進行校驗的運算，以保證檔案與資料確實是由原創者所提供
SRS-05	資料傳輸過程會使用安全的協定，防止資料被竄改
SRS-06	本產品之輸入驗證會採用過濾機制，以防止輸入惡意的命令或資料
SRS-07	本產品會對使用者輸入之資料進行驗證
SRS-08	本產品對於產生之參數會判斷其合理性，例如:LED燈亮之間隔
SRS-09	本產品身分認證發生錯誤時，預設不允許存取任何功能
SRS-10	本產品執行功能或存取資源前，會檢查是否經過使用者的授權
SRS-11	本產品之使用者賦予所需的最小權限
SRS-12	本產品之服務程序以最小的權限執行，不以系統管理員或最高權限執行
SRS-13	在系統存取失敗、資料傳輸失敗、重要資料異動、功能錯誤及管理者行為都會進行記錄，本產品會將這些Log紀錄存放於手機與伺服器端
SRS-14	本產品功能在發生錯誤時會進行錯誤及例外處理，此錯誤及例外處理會將產品之正確資訊釋放
SRS-15	本產品所依賴之外部元件與軟體，不會使用預設之帳號與密碼
SRS-16	本產品所使用之作業平台會定期進行更新、關閉不必要服務、並注意安全之設定
SRS-17	本產品所依賴之外部元件與軟體，會注意其安全漏洞通告，必要時進行評估並更新

2.3 網路安全細部設計(Security Detail Design, SDD)

本產品網路安全細部設計(Security Detail Design, SDD) 如下表2.3.1，根據SRS的要求落實於產品，確認本產品之網路安全要求。

表2.3.1、網路安全細部設計

SDD編號 No. (SDD)	網路安全設計規格說明(Security Detail Design, SDD Description)
SDD-01	資料傳輸前，需做AES128 加密
SDD-02	資料儲存時，需做AES128加密進行儲存
SDD-03	重要資料在接收時使用雜湊(HASH)作為檔案校驗碼進行驗證
SDD-04	資料傳輸過程會使用安全通訊加密的協定(SSL)
SDD-05	輸入驗證會採用過濾機制過濾惡意命令、驗證使用者輸入的資料、並檢查參數的合理性
SDD-06	本產品會對使用者輸入資料及設定進行驗證，並判斷其合理性
SDD-07	本產品經過手機端軟體使用者授權確認後，手機應用程式可接收手錶端傳輸之資料並顯示
SDD-08	本產品對使用者僅開放最小使用權限，身分認證發生錯誤時，預設不允許存取任何功能
SDD-09	運行時不開啟任何系統管理員的相關功能，包括校準參數、log檔查詢/修改等。
SDD-10	在系統存取失敗、資料傳輸失敗、重要資料異動、功能錯誤及管理者行為都會進行記錄，本產品會將這些Log紀錄存放於手機與伺服器端
SDD-11	本產品功能在發生錯誤時會進行錯誤及例外處理，此錯誤及例外處理會將產品之正確資訊釋放
SDD-12	本產品所依賴之外部元件與軟體，不會使用預設之帳號與密碼
SDD-13	本產品所使用之作業平台會定期進行更新、關閉不必要服務、並注意安全之設定
SDD-14	本產品所依賴之外部元件與軟體，會注意其安全漏洞通告，必要時進行評估並更新

2.4 網路安全驗證確效測試(Security Validation & Verification, SVV)

表2.4.1到表2.4.15為ABC血氧濃度應用軟體網路安全驗證確效測試表格。

表2.4.1、網路安全驗證確效測試(測試1)

測試編號	SVV-01
軟體版本	1.0.0
測試項目	血氧量測資料傳送時需採用加密通訊協定
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	傳輸的封包為亂碼，經進階加密標準(Advanced Encryption Standard 128 Bit, AES128) 解開後呈現明碼。

測試結果	Pass

表2.4.2、網路安全驗證確效(測試2)

測試編號	SVV-02
軟體版本	1.0.0
測試項目	血氧量測資料接收端儲存資料時會做加密處理
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	ABC血氧濃度應用軟體系統中的資料經工具驗證使用進階加密標準(Advanced Encryption Standard 128 Bit, AES128) 儲存。
測試結果	Pass

表2.4.3、網路安全驗證確效(測試3)

測試編號	SVV-03
軟體版本	1.0.0
測試項目	血氧量測資料傳送、儲存時，不使用自行創造的加密方式
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	1. 傳輸的封包為亂碼，經進階加密標準(Advanced Encryption Standard 128 Bit, AES128) 解開後呈現明碼。 2. ABC血氧濃度應用軟體系統中的資料經工具驗證使用進階加密標準(Advanced Encryption Standard 128 Bit, AES128) 儲存。
測試結果	Pass

表2.4.4、網路安全驗證確效(測試4)

測試編號	SVV-04
軟體版本	1.0.0
測試項目	血氧量測資料會使用雜湊(HASH)進行校驗的運算，以保證檔案與資料確實是由原創者所提供
測試人員	呂OO
測試日期	2021/11/30

測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	手機端接收檔案後，進行雜湊(HASH)校驗，以保證檔案與資料確實是由信賴來源所提供。
測試結果	Pass

表2.4.5、網路安全驗證確效(測試5)

測試編號	SVV-05
軟體版本	1.0.0
測試項目	資料傳輸過程會使用安全的協定，防止資料被竄改
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	手機端與手錶端運用安全套接層協議（Secure Socket Layer, SSL）加密傳輸可正常連線、傳輸資料。
測試結果	Pass

表2.4.6、網路安全驗證確效(測試6)

測試編號	SVV-06
軟體版本	1.0.0
測試項目	本產品之輸入驗證會採過濾機制，以防止輸入惡意的命令或資料
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	設定惡意命令或資料辭庫，過濾使用者輸入的惡意命令或資料；輸入正確資訊後，回傳伺服器，伺服器能正確接收資訊。
測試結果	Pass

表2.4.7、網路安全驗證確效(測試7)

測試編號	SVV-07
軟體版本	1.0.0
測試項目	本產品會對使用者輸入之資料進行驗證
測試人員	呂OO
測試日期	2021/11/30

測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	1. 使用者輸入不合產品設定資料，系統不接受輸入結果並顯示錯誤訊息 2. 使用者輸入錯誤產品數值範圍，系統不接受輸入結果並顯示錯誤訊息
測試結果	Pass

表2.4.8、網路安全驗證確效(測試8)

測試編號	SVV-08
軟體版本	1.0.0
測試項目	本產品對於產生之參數會判斷其合理性，例如:LED燈亮之間隔
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	進行系統設定時輸入錯誤數值，程式回報錯誤並顯示參數錯誤訊息
測試結果	Pass

表2.4.9、網路安全驗證確效(測試9)

測試編號	SVV-09
軟體版本	1.0.0
測試項目	本產品執行功能或存取資源前，會檢查是否經過使用者的授權
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	經過手機端軟體使用者授權確認後，手機應用程式可接收手錶端傳輸之資料並顯示
測試結果	Pass

表2.4.10、網路安全驗證確效測試(測試10)

測試編號	SVV-10
軟體版本	1.0.0
測試項目	本產品對使用者僅開放最小使用權限，身分認證發生錯誤時，預設不允許存取任何功能

測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	以使用者帳號登錄後，只能使用一般產品功能，無法關閉系統相關功能、修改測量參數等行為。
測試結果	Pass

表2.4.11、網路安全驗證確效測試(測試11)

測試編號	SVV-11
軟體版本	1.0.0
測試項目	本產品之服務程序以最小的權限執行，不以系統管理員或最高權限執行
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	產品與手錶於運行時不開啟任何系統管理員的相關功能，包括校準參數、log檔查詢/修改等。
測試結果	Pass

表2.4.12、網路安全驗證確效測試(測試12)

測試編號	SVV-12
軟體版本	1.0.0
測試項目	在系統存取失敗、資料傳輸失敗、重要資料異動、功能錯誤及管理者行為都會進行記錄，本產品會將這些Log紀錄存放於手機與伺服器端
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	使用者對於產品的任何操作如產品資料儲存、刪除、傳輸等皆會記綠於log檔中
測試結果	Pass

表2.4.13、網路安全驗證確效測試(測試13)

測試編號	SVV-13
軟體版本	1.0.0

測試項目	本產品功能在發生錯誤時會進行錯誤及例外處理，此錯誤及例外處理會將產品之正確資訊釋放
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	當系統發生如故障、資料傳輸連線中斷或是封包遺失等錯誤狀況發生時能自動修復產品確保功能重新正常運作
測試結果	Pass

表2.4.14、網路安全驗證確效測試(測試14)

測試編號	SVV-14
軟體版本	1.0.0
測試項目	本產品所依賴之外部元件與軟體，不會使用預設之帳號與密碼
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	本產品所使用的外部元件與軟體都不使用預設帳號與密碼
測試結果	Pass

表2.4.15、網路安全驗證確效測試(測試15)

測試編號	SVV-15
軟體版本	1.0.0
測試項目	本產品所使用之作業平台會定期進行更新、關閉不必要服務、並注意安全之設定
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	產品的作業平台會定期與伺服器端更新並檢查系統安全設定與關閉不必要的服務
測試結果	Pass

表2.4.16、網路安全驗證確效測試(測試16)

測試編號	SVV-16

軟體版本	1.0.0
測試項目	本產品所依賴之外部元件與軟體，會注意其安全漏洞通告，必要時進行評估並更新
測試人員	呂OO
測試日期	2021/11/30
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	依據網路安全制定計畫，適時追蹤使用者的產品版本，並在有安全漏洞發生時推行版本更新
測試結果	Pass

2.5 追溯性矩陣(Traceability Matrix)

錯誤! 找不到參照來源。為ABC血氧濃度應用軟體之追溯性矩陣。

表2.5.1、追溯性矩陣範例

軟體需求編號	軟體設計規格編號	軟體 V&V 測試編號
SRS-01	SDD-01	SVV-01
SRS-02	SDD-02	SVV-02
SRS-03	SDD-01、SDD-02	SVV-03
SRS-04	SDD-03	SVV-04
SRS-05	SDD-04	SVV-05
SRS-06	SDD-05	SVV-06
SRS-07	SDD-06	SVV-07
SRS-08	SDD-06	SVV-08
SRS-09	SDD-08	SVV-10
SRS-10	SDD-07	SVV-09
SRS-11	SDD-08	SVV-10
SRS-12	SDD-09	SVV-11
SRS-13	SDD-10	SVV-12
SRS-14	SDD-11	SVV-13
SRS-15	SDD-12	SVV-14
SRS-16	SDD-13	SVV-15
SRS-17	SDD-14	SVV-16

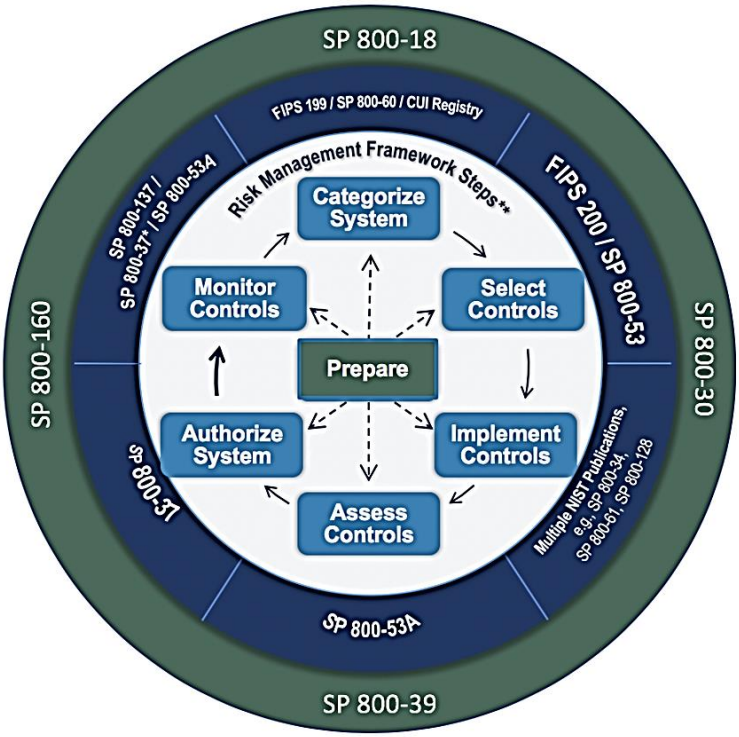
3. 網路安全評估(Cybersecurity Assessment)

3.1 網路安全評估計畫(Cybersecurity Assessment Plan)

本產品參照NIST SP 800標準，針對產品進行：

- 本產品軟硬體元件之盤點與分類
- 本產品之網路安全威脅建模
- 本產品之網路安全風險評估
- 本產品之網路安全風險控制措施
- 本產品之網路安全檢測與報告

- [SP 800-30] provides guidance on the risk assessment process.
- [IR 8062] introduces privacy risk concepts.
- [SP 800-39] provides guidance on risk management processes and strategies.
- [SP 800-37] provides a comprehensive risk management process.
- [SP 800-53A] provides guidance on assessing the effectiveness of controls.
- [SP 800-53B] provides guidance for tailoring security and privacy control baselines and for developing overlays to support the specific protection needs and requirements of stakeholders and their organizations.



3.1.1 網路安全威脅建模方法(Security Requirement Specification & Threat Modeling)

網路安全威脅建模包括：

1 識別資產

2 產生資料流向圖（Data Flow Diagram, DFD）

3 分析網路安全威脅。在DFD中每一類部件都有對應STRIDE [假冒（Spoofing）、篡改（Tampering）、否認性（Repudiation）、資訊泄露（Information disclosure）、阻斷服務（Denial of service）、權限提高（Elevation of privilege）]模型威脅。輸出威脅列表，對每個威脅項進行評估處理。

3.1.2 識別資產(Assets Identification)

針對系統的資產識別，可以將系統資產加以分類：

表3.1.2.1、識別資產分類描述

分類	描述
機敏資料	任何資料其機密性、完整性、可用性遭到破壞時，將會遭受重大不利影響者，如系統組態檔
外部實體	驅動軟體的某人或某物，且為軟體本身無法控制者
程序	處理輸入資料的工作或行為，並輸出資料者，如作業系統、韌體
資料流	資料於軟體或系統中移動的方法，如通訊協定
資料儲存庫	軟體中資料暫時或持續的儲存區，如日誌資料

表3.1.2.2、ABC血氧濃度應用軟體識別資產

分類	資產名稱	描述
機敏資料	血氧濃度量測數據	病患血氧濃度量測數據
機敏資料	系統組態檔	包括血氧參數等系統參數設定檔與網路傳輸相關設定檔
外部實體	使用者	系統的使用者
程序	手錶/APP操作介面	手錶上即時血氧濃度顯示介面與APP血氧濃度變化監控畫面
資料流	藍芽通訊協定	APP與手機間使用藍芽通訊協定傳輸資料
資料儲存庫	日誌資料	手錶操作紀錄檔案與系統log

3.2 資料流向圖(Data Flow Diagram, DFD)

表3.2.1、資料分級之參考

資料安全等級	等級	資安防護特性		
		機密性	完整性	可用性
	高	只有限制性的系統角色才能揭露資料	資料遭到竄改會造成嚴重危害	資料遭到毀壞會造成嚴重危害
	中	系統角色可揭露資料	資料遭到竄改會造成中度危害	資料遭到毀壞會造成中度危害
	低	資料可以公開揭露	資料遭到竄改會造成輕度危害	資料遭到毀壞會造成輕度危害

本產品使用案例如下圖所示：

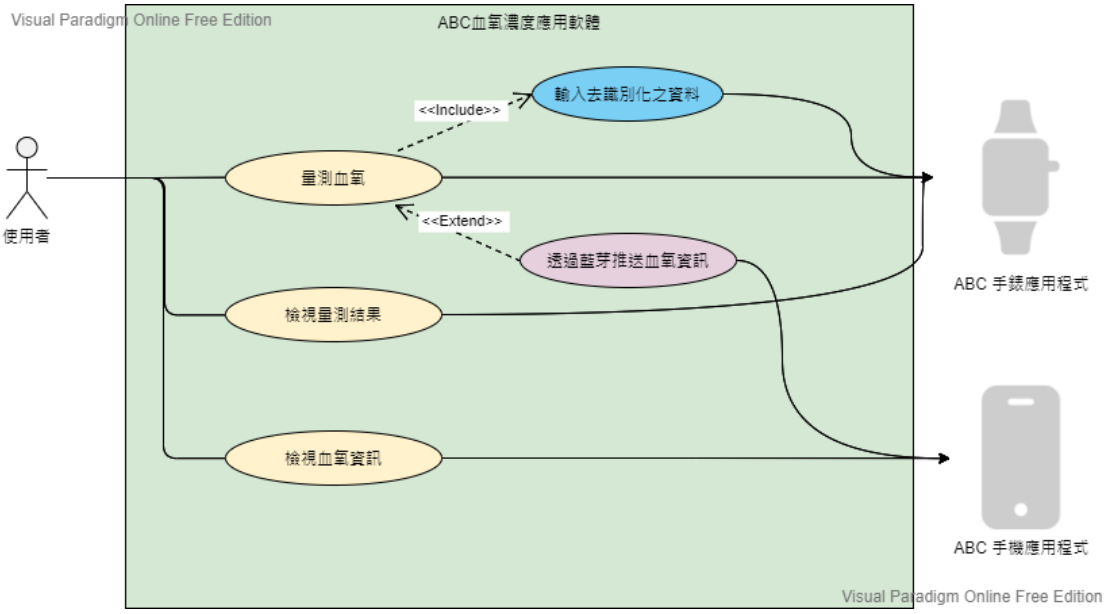


圖3.2.1、ABC血氧濃度應用軟體使用案例圖

以從資料的角度來描述一個系統。元素如下：

- Flow( )
- File/Database ( )：表示文件、資料庫
- Function（ ）
- Input/Output（ ）：系統的端點，例如人。
- 信任邊界（ ）：表示可信元素與不可信元素之間的邊界。

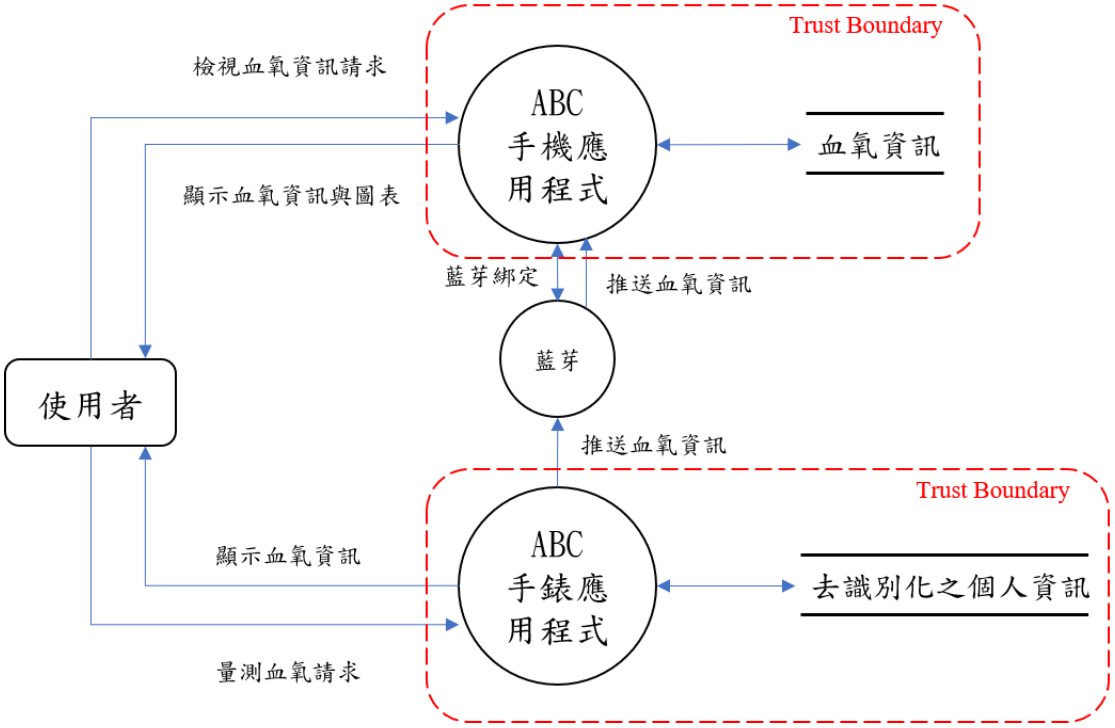


圖3.2.2、ABC血氧濃度應用軟體資料流向圖

3.3 分析網路安全威脅(Cybersecurity Threat Analysis)

表3.3.1、STRIDE模型之類別說明

類別	描述	資安防護特性
假冒 (Spoofing)	涉及非法存取然後使用其他使用者的驗證資訊，例如使用者名稱和密碼。	身分認證 (Authentication)
竄改 (Tampering)	涉及惡意修改資料。例如在未經授權的狀況下變更資料庫中保存的持續性資料，以及修改在兩部電腦之間透過開放式網路(例如網際網路) 流動的資料。	完整性 (Integrity)
否認性 (Repudiation)	與拒絕執行動作但沒有其他任何一方有辦法另外證明的使用者有關，例如使用者在無法追蹤違禁作業的系統中執行非法作業。不可否認性是指系統對抗否認性威脅的能力。概念近似於購買商品的使用者可能必須在收到商品時簽名。然後，廠商可以使用簽名收據做為使用者已收到包裹的證據。	不可否認性 (Non-repudiation)
資訊洩漏 (Information Disclosure)	涉及將資訊暴露給不應具有其存取權的個人，例如，使用者可以讀取其未被授權可存取的檔案，或入侵者能夠讀取在兩部電腦之間傳輸的資料。	機密性 (Confidentiality)

阻斷服務(Denial of Service, DoS)	阻斷服務攻擊可阻斷對有效使用者提供的服務，例如，藉由讓網頁伺服器暫時無法存取或無法使用。您必須防止特定類型的DoS威脅，以便提升系統的可取得性和可靠性(availability and reliability)。	可用性(Availability)
權限提高(Elevation of Privilege)	未授權的使用者取得授權的存取權，因此有足夠存取權危害或摧毀整個系統。提高權限威脅包含攻擊者已有效地滲透所有系統防禦，並成為受信任系統本身的一部分，這確實是危險的情況。	授權(Authorization)

表3.3.2、風險降低類別[3]

類別	描述
稽核和記錄	誰在何時做了什麼？稽核和記錄是指應用程式記錄安全性相關事件的方式
驗證	您是誰？驗證是某實體證明另一個實體身分識別的程序 (通常透過使用者名稱和密碼等認證)
授權	您可以做什麼授權是應用程式針對資源和作業提供存取控制的方式
通訊安全性	您在與誰對話？通訊安全性可確保所有通訊是在最安全的情況下進行的
組態管理	應用程式的執行身分為何其所連線到的資料庫為何？應用程式的管理方式為何如何保護這些設定？ 組態管理指的是應用程式處理這些作業問題的方式
密碼編譯	如何保護機密資料(機密性)？如何防止資料或程式庫遭到竄改(完整性)如何為必須是密碼編譯增強式的隨機值提供種子？密碼編譯是指應用程式強制執行機密性與完整性的方式
例外狀況管理	當應用程式中的呼叫失敗時，應用程式會如何處理？ 您要顯示多少資料？您要對使用者傳回容易理解的錯誤資訊嗎？ 您要將重要例外狀況資訊傳回給呼叫者嗎？應用程式會呼叫失敗嗎？
輸入驗證	您如何知道應用程式收到的輸入是有效且安全的？ 輸入驗證指的是應用程式如何先篩選、消除或拒絕輸入再進行其他處理。請考慮透過進入點限制輸入並透過退出點編碼輸出。您是否信任來源的資料，例如來自資料庫和檔案共用？
機敏性資料	應用程式如何處理機敏性資料？ 機敏性資料指的是應用程式如何處理記憶體中、透過網路或持續性存放區中必須受到保護的任何資料

[3] Microsoft 威脅模型化工具風險降低. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-mitigations

會話管理	應用程式如何處理和保護使用者工作階段？ 工作階段是指使用者與 Web 應用程式之間的一系列相關互動

表3.3.3、網路安全威脅分析表

資產名稱	假冒(S)	竄改(T)	否認行為(R)	資訊洩露(I)	拒絕存取服務(D)	權限提高(E)	威脅列表
作業系統					V		D1：透過入侵作業系統關閉相關服務或應用系統
韌體		V		V			T1：內部不法人員竄改韌體，植入相關木馬或後門程式 I1：透過韌體的偵測或側錄，揭露資訊
系統組態檔		V			V		T2：透過組態設定變更，更改系統服務。 D2：透過組態設定開啟相關通訊介面，以揭露資訊。
機敏性資料				V			I2：針對未保護的機敏性資料進行揭露
日誌資料		V					T3：竄改日誌資料，隱匿不法行為
通訊協定	V			V			S1：透過重送攻擊來進行假冒攻擊 I2：針對未保護的通訊管道揭露資訊
操作介面					V		D3：關閉顯示與測量功能，讓使用者無法正常使用APP與手錶相關功能

基於STRIDE與DFD結果，便可以針對系統組成元素分析其網路安全威脅，以及可能的攻擊樹(Attack Tree)，如下圖3.3.1所示：

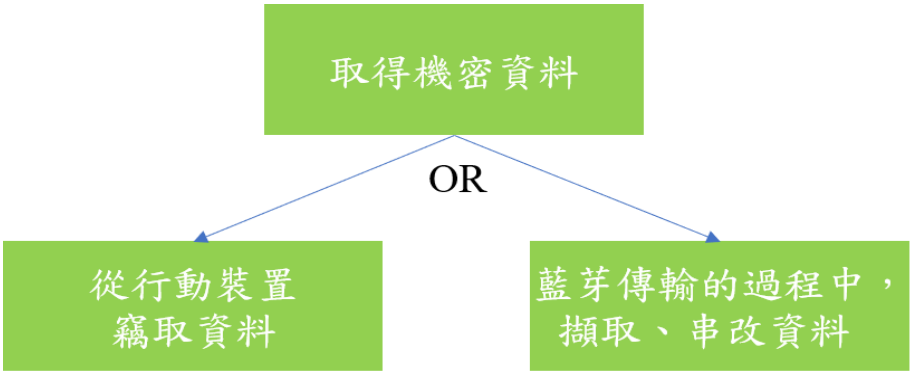


圖3.3.1、攻擊樹狀圖簡單案例圖

3.4 網路安全風險評鑑方法(Cybersecurity Risk Assessment Methodology)

醫療器材的風險評鑑方法，可以參考醫療器材的網路安全風險評鑑框架：

1. 識別威脅來源與弱點
2. 網路安全威脅/風險情境分析
3. 可用性評估
4. 影響性評估
5. 風險評分
6. 風險管理與控制措施

上述步驟1 (識別威脅來源與弱點)以及步驟2 (網路安全風險情境分析)即為第2.2.4節分析網路安全威脅的結果。本章節主要來針對前述網路安全威脅列表的所有威脅進行各別的網路安全風險評鑑。醫療器材之網路安全風險因素主要可分為以下兩種，詳細網路安全因素與風險值由表3.4.1所示：

- 威脅(外部因素)：主要從攻擊者的角度，來探討其針對醫療器材造成網路安全威脅的風險狀況，其評估因子有技能等級、動機、機會與資源3項。
- 弱點(內部因素)：主要從防禦方以及醫療器材本身的安全漏洞，來探討醫療器材之網路安全漏洞可被利用而造成網路安全風險的狀況，其評估因子有發現難易度、可用性與入侵偵測3項。

威脅來源可能來自於使用者、維護廠商、醫院醫工、其他可能碰觸者或網路惡意攻擊者。

表3.4.1、表3.4.2、表3.4.3分別描述了影響醫療器材網路安全的可用性、影響性與發生可能性的相關數值，並經由表3.4.4中的計算公式，將上述所提及的數值合併成代表醫療器材的整體風險值。

表3.4.1、醫療器材的網路安全因素與風險值[4]

可利用性	Threat Agent Factors 威脅因素			Vulnerability Factors 弱點因素		
風險因素與風險值	**T1** Skill level 技能等級	**T2** Motive 動機	**T3** Opportunity & Resources 機會與資源	**V1** Ease of Discovery & Awareness 發現的難易度	**V2** Ease of Exploiting 可用性	**V3** Intrusion Detection 入侵偵測
說明	**就已知現狀電腦技能選最高**	**資料有價值或量大可轉賣獲利/新上市高貴儀器可出名**	**權限管理、實體環境/系統運作介面之控管**	**視使用作業系統，若為主流設備(設備市佔高)或作業系統廠商較能支援**	**若為主流作業系統, 網路上可搜尋到較多的入侵工具**	**是否有安全偵測、有入侵日誌、能自動偵側**
1	無技術性技能或具一般電腦能力	低度或無獎勵或無誘因, 如無個資為	實體環境/系統運作介面有加以控管	1.設備市佔高或設備之作業系統為大宗,	非大宗、非主流作業系統或設備市佔	有檢附防護機制或人員對入

[4] 行政院衛生福利部關鍵基礎設施資安工作推動專案辦公室. 醫療器材的網路安全因素與風險值.

		一般性設備	且有特殊權限	廠商能支援程式修補, 2.作業系統客製化攻擊意願較低	低，網路入侵工具較少	侵能即時偵測
2	具備部分技術性技能或具備網路與程式撰寫能力	可能有獎勵與誘因, 如檢查量大設備且有醫療資訊	僅有權限管理但無實際人員/角色管理	使用的作業系統非大宗或較舊作業系統 但廠商仍支援程式修補	使用的作業系統非大宗或較舊作業系統，但網路入侵仍有工具	人員對入侵後知後覺
3	具備資安滲透技能	高度獎勵與誘因, 如攻擊尖端設備可成名, 或取得具價值的醫療資訊	實體環境/系統運作介面有加以控管，但不需任何權限或資源可達成入侵目的	舊作業系統之弱點廠商已不支援程式修補	設備市佔高、設備作業系統為大宗或主流，網路入侵工具較多	人員對入侵不知不覺

表3.4.2、醫療器材網路安全風險的影響等級

影響等級	嚴重程度
說明	**病人安全影響的嚴重程度**
1	無損害或造成病人不方便之情形
2	間接傷害，指當下未造成病人直接傷害但病人有潛在傷害的風險
3	直接傷害，指當下即造成病人的損傷或傷害，嚴重者可能追成病人死亡

表3.4.3、醫療器材網路安全風險的發生可能性數值

發生可能性數值	可能由插槽/系統運作介面遭受的風險機會
1	設備無插槽另提供外接或 設備有插槽且有使用者管控措施
2	設備有插槽但無使用者管控措施

表3.4.4、醫療器材風險值的計算

風險值	**風險值 ＝可用性風險值 × 影響性風險值 × 發生可能性數值** （風險值最高值為 18，最低值為 1）
	● 可用性風險值 = 6項風險因素值的平均 (1~3) ● 影響性風險值 = 病人安全影響程度風險值 (1~3) ● 發生可能性數值= 可能由插槽/系統運作介面遭受的風險機會 (1~2)
風險等級	● **A級(高風險)**：風險值介於13.0 ~ 18.0 ，**不可接受(Unacceptable)** ● **B級(中風險)**：風險值介於7.0 ~ 12.9，**可能接受的(Potentially Acceptable)** ● **C級(低風險)**：風險值介於1.0 ~ 6.9，**可接受的(Acceptable)**

表3.4.5、醫療器材網路安全風險等級檢核表

醫療器材組成元件	威脅類型	(I) Impact factor 影響程度 (低:1~高:3)	可利用性						(R) 風險值 (低：1~高：3)	(P) 發生可能性 (低：1~高：2)	(E) 風險結果	(R) 風險等級 A:高風險 (不可接受) B:中風險 (可能接受的) C:低風險 (可接受)	風險編號	風險控制措施
			(T) Threat Agent Factors 威脅因素 (低：1~高：3)			(V) Vulnerability Factors 弱點因素 (低：1~高：3)								
元件	威脅	病人危害程等	(T1) 技能等級	(T2) 動機	(T3) 機會與資源	(V1) 發現的難易度	(V2) 可用性	(V3) 入侵偵測	R=avg(T+V) 平均值	由插槽/系統運作介面遭遇的風險機會	I*R*P	A:13~18 B:7.0~12.9 C:1.0~6.9	風險	控制措施
作業系統	D1	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-01	SDD-08: 給予使用者操作時所需最低權限
韌體	T1	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-02	SDD-07: 本產品之服務程序以最小的權限執行，不以系統管理員或最高權限執行
韌體	I1	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-03	SDD-03: 使用安全通訊加密

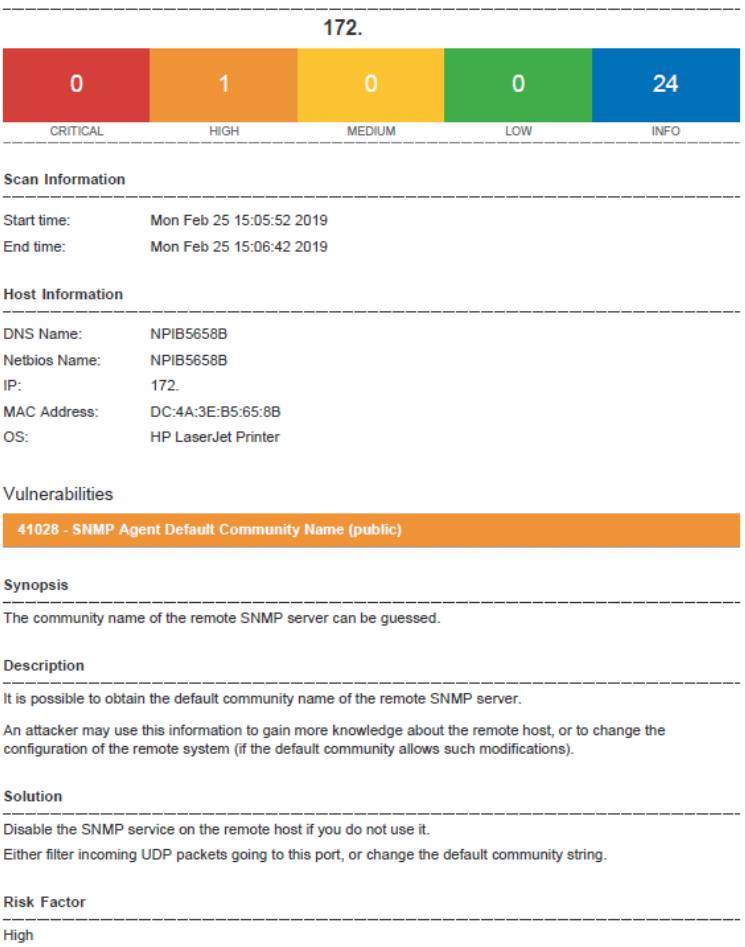
													的協定
系統組態檔	T2	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-04	SDD-07: 本產品之服務程序以最小的權限執行，不以系統管理員或最高權限執行
系統組態檔	D2	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-05	SDD-07: 本產品之服務程序以最小的權限執行，不以系統管理員或最高權限執行
機敏性資料	I2	1	3	1	1	1	2	3	1.83	1	1.83	低風險(可接受)	Risk-06	SDD-02:使用AES128加密儲存
日誌資料	T3	1	3	1	1	1	2	2	1.67	1	1.67	低風險(可接受)	Risk-07	SDD-09: 於伺服器端會有一Log記錄所有對於本系統進行的行為
通訊協定	S1	1	3	1	1	1	2	3	1.83	2	3.67	低風險(可接受)	Risk-08	SDD-05: 輸入驗證

通訊協定	I3	1	3	1	1	1	2	3	1.83	2	3.67	低風險(可接受)	Risk-09	SDD-03: 使用安全通訊加密的協定
操作介面	D3	1	3	2	1	1	2	2	1.83	2	3.67	低風險(可接受)	Risk-10	SDD-08: 給予使用者操作時所需最低權限

3.5 網路安全檢測方法(Cybersecurity Testing Methodology)

3.5.1 漏洞掃描(Vulnerability Scanning)

漏洞掃描是針對已知的系統漏洞，對該系統進行掃描、攻擊、測試。漏洞掃描可瞭解現有環境中各種網路設備、系統與主機所存在之漏洞狀況，並透過漏洞掃描結果分析報告獲得有效的改善方案。漏洞通常因缺陷 (flaws) 或錯誤配置(misconfigurations)而產生。缺陷是由產品的設計缺陷造成，常見軟體缺陷是緩衝區溢出(buffer overflow)。錯誤配置例如薄弱的錯誤配置存取控制表、開放的埠和不必要的服務，OWASP網站(https://owasp.org/www-community/Vulnerability_Scanning_Tools)列舉漏洞掃描工具可供參考。



172.

0	1	0	0	24
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Feb 25 15:05:52 2019
End time: Mon Feb 25 15:06:42 2019

Host Information

DNS Name: NPIB5658B
Netbios Name: NPIB5658B
IP: 172.
MAC Address: DC:4A:3E:B5:65:8B
OS: HP LaserJet Printer

Vulnerabilities

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

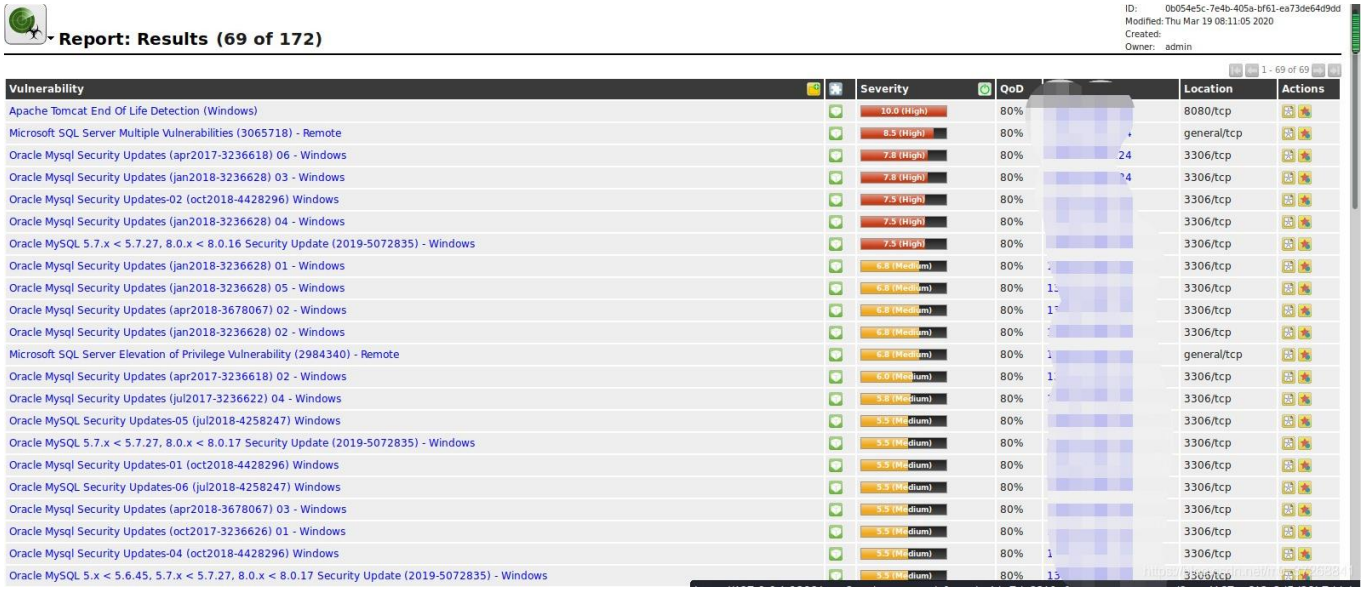
Risk Factor

High

圖3.5.1.1、漏洞掃描測試報告範例

3.5.2 滲透測試(Penetration Testing)

滲透測試(Penetration Test)通常是由資安團隊以駭客之思維與行為模式規劃測試內容，利用漏洞掃描軟體或其他的工具，從外部和內部網路進行模擬入侵，收集系統的相關資訊，探查漏洞。



Report: Results (69 of 172)

ID: 0b054e5c-7e4b-405a-bf61-ea73de64d9dd
Modified: Thu Mar 19 08:11:05 2020
Created:
Owner: admin

1 - 69 of 69

Vulnerability	Severity	QoD	Location	Actions
Apache Tomcat End Of Life Detection (Windows)	10.0 (High)	80%	8080/tcp	
Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote	8.5 (High)	80%	general/tcp	
Oracle Mysql Security Updates (apr2017-3236618) 06 - Windows	7.8 (High)	80%	3306/tcp	
Oracle Mysql Security Updates (jan2018-3236628) 03 - Windows	7.8 (High)	80%	3306/tcp	
Oracle Mysql Security Updates-02 (oct2018-4428296) Windows	7.5 (High)	80%	3306/tcp	
Oracle Mysql Security Updates (jan2018-3236628) 04 - Windows	7.5 (High)	80%	3306/tcp	
Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.16 Security Update (2019-5072835) - Windows	7.5 (High)	80%	3306/tcp	
Oracle Mysql Security Updates (jan2018-3236628) 01 - Windows	6.8 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (jan2018-3236628) 05 - Windows	6.8 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (apr2018-3678067) 02 - Windows	6.8 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (jan2018-3236628) 02 - Windows	6.8 (Medium)	80%	3306/tcp	
Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote	6.8 (Medium)	80%	general/tcp	
Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows	6.0 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (jul2017-3236622) 04 - Windows	5.8 (Medium)	80%	3306/tcp	
Oracle MySQL Security Updates-05 (jul2018-4258247) Windows	5.5 (Medium)	80%	3306/tcp	
Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072835) - Windows	5.5 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates-01 (oct2018-4428296) Windows	5.5 (Medium)	80%	3306/tcp	
Oracle MySQL Security Updates-06 (jul2018-4258247) Windows	5.5 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (apr2018-3678067) 03 - Windows	5.5 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates (oct2017-3236626) 01 - Windows	5.5 (Medium)	80%	3306/tcp	
Oracle Mysql Security Updates-04 (oct2018-4428296) Windows	5.5 (Medium)	80%	3306/tcp	
Oracle MySQL 5.x < 5.6.45, 5.7.x < 5.7.27, 8.0.x < 8.0.17 Security Update (2019-5072835) - Windows	5.5 (Medium)	80%	3306/tcp	

圖3.5.2.1、滲透測試報告範例圖

附錄一：醫療器材網路安全評估—自我檢核表(Cybersecurity Self-Checklist)

使用附件“醫療器材網路安全之業者揭露聲明書”檔案

附錄二：本產品相關醫療器材之網路安全通報 (Related Cybersecurity Alerts)

調查並呈現相關醫療器材網路安全通知、漏洞資料庫資訊及產品應對措施。

表1呈現美敦力之 MiniMed 於美國國家漏洞資料庫的資訊，圖1以CVE-2019-10964 為例呈現評估。

表1、MiniMed 於美國國家漏洞資料庫的資訊(關鍵字: MiniMed)

漏洞編號	說明
CVE-2019-10964	In Medtronic MinMed 508 and Medtronic Minimed Paradigm Insulin Pumps, Versions, MiniMed 508 pump – All versions, MiniMed Paradigm 511 pump – All versions, MiniMed Paradigm 512/712 pumps – All versions, MiniMed Paradigm 712E pump–All versions, MiniMed Paradigm 515/715 pumps–All versions, MiniMed Paradigm 522/722 pumps – All versions,MiniMed Paradigm 522K/722K pumps – All versions, MiniMed Paradigm 523/723 pumps – Software versions 2.4A or lower, MiniMed Paradigm 523K/723K pumps – Software, versions 2.4A or lower, MiniMed Paradigm Veo 554/754 pumps – Software versions 2.6A or lower, MiniMed Paradigm Veo 554CM and 754CM models only – Software versions 2.7A or lower, the affected insulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with adjacent access to one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery. **Published:** June 28, 2019; 5:15:11 PM -0400 V3.0:**8.8 HIGH** V2.0:**5.8 MEDIUM**
CVE-2018-14781	Medtronic MMT 508 MiniMed insulin pump, 522 / MMT - 722 Paradigm REAL-TIME, 523 / MMT - 723 Paradigm Revel, 523K / MMT - 723K Paradigm Revel, and 551 / MMT - 751 MiniMed 530G The models identified above, when paired with a remote controller and having the "easy bolus" and "remote bolus" options enabled (non-default), are vulnerable to a capture-replay attack. An attacker can capture the wireless transmissions between the remote controller and the pump and replay them to cause an insulin (bolus) delivery. **Published:** August 13, 2018; 5:48:01 PM -0400 V3.0:**5.3 MEDIUM**

	V2.0:**2.9 LOW**
CVE-2018-10634	Medtronic MMT 508 MiniMed insulin pump, 522 / MMT - 722 Paradigm REAL-TIME, 523 / MMT - 723 Paradigm Revel, 523K / MMT - 723K Paradigm Revel, and 551 / MMT - 751 MiniMed 530G communications between the pump and wireless accessories are transmitted in cleartext. A sufficiently skilled attacker could capture these transmissions and extract sensitive information, such as device serial numbers. **Published:** August 13, 2018; 5:47:59 V3.0:**5.3 MEDIUM** V2.0:**2.9 LOW**

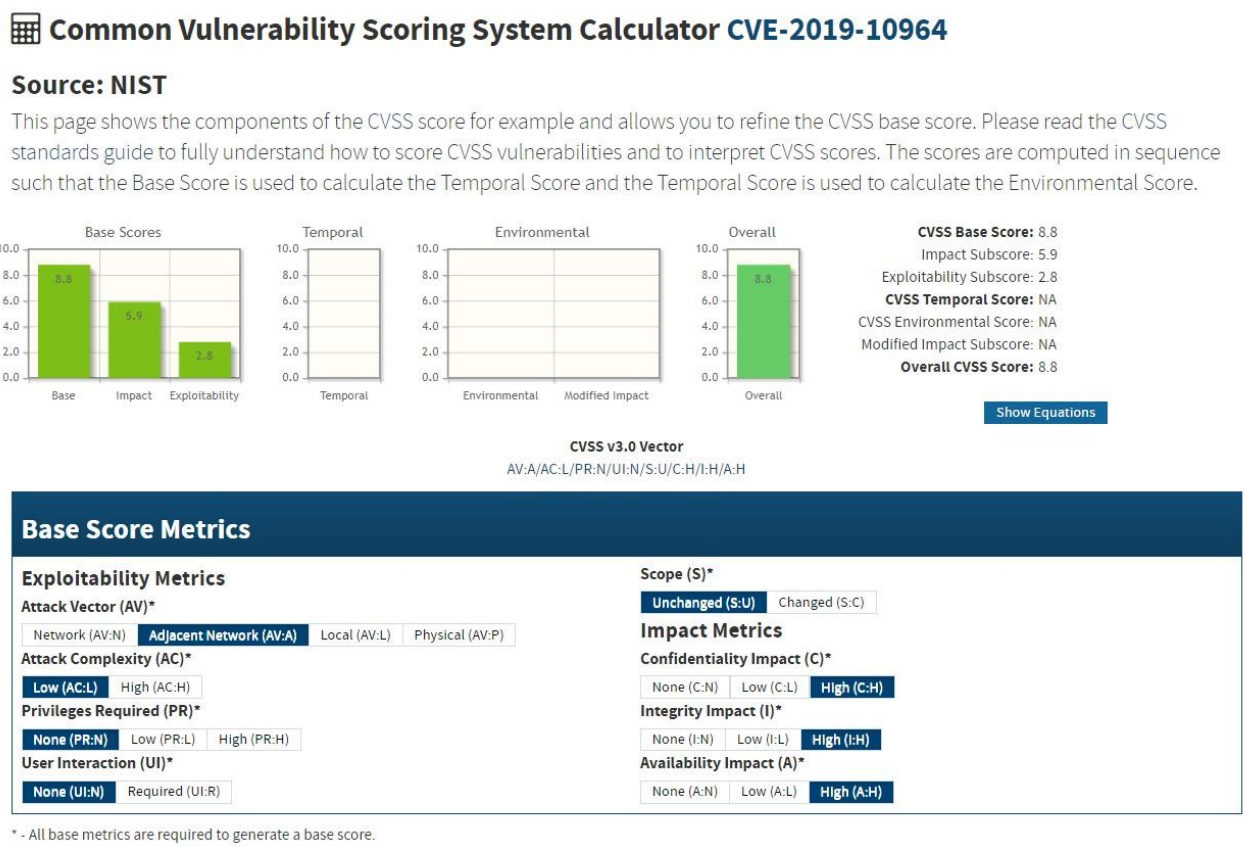


圖1、CVE-2019-10964 之 CVSS v3.0 評估

本章節彙整 2013~2020 年間美國FDA 網路安全通知(詳如表2)[5,6]。

表2、美國FDA 網路安全通知彙整(2013~2020 年)

日期	安全通知	描述
2020/03/03	SweynTooth 網路安全漏洞可能會影響某些醫療器材	FDA通知患者、醫療保健提供者和製造廠有關SweynTooth系列網路安全漏洞的訊息，這些漏洞可能會給某些醫療器材帶來風險。
2020/01/23	GE Healthcare 臨床資訊中央工作站和遠端伺服器的網路安全漏洞	FDA 正在提高醫療保健供應商和醫療機構工作人員的意識，即某些 GE Healthcare 臨床資訊中央工作站和遠端伺服器中的網路安全漏洞可能會在受到監視的同時給患者帶來風險。
2019/10/01	URGENT/11 網路安全漏洞可能會在使用某些醫療器材時引入風險	FDA 正在就連網醫療器材和醫療保健網路的網路安全漏洞向患者、醫療服務提供者、醫療設施工作人員和製造廠提供資訊。
2019/06/27	某些Medtronic MiniMed胰素幫浦具有潛在的網路安全風險	FDA 已經意識到某些 Medtronic MiniMed Paradigm 胰島素幫浦的潛在網路安全風險。FDA 建議患者使用性能更好的型號替換受影響的幫浦，以保護他們免受這些潛在風險的影

[5] https://www.accessdata.fda.gov/cdrh_docs/pdf/P980016S436M.pdf
[6] https://www.fda.gov/medical-devices/digital-health/cybersecurity#safety

		響。
2015/05/13	Hospira 的 LifeCare PCA3 和 PCA5 輸液幫浦系統-資訊安全漏洞	在獨立研究人員發布有關這些漏洞的資訊後，FDA 和 Hospira 意識到了這些輸液系統中的網路安全漏洞。2015年 7 月 31 日，Hospira 和一名獨立研究人員確認可以使用 Symbiq Infusion System 通過醫院網路遠端存取。
2013/6/13	醫療器材和醫院網路的網路安全	FDA 建議醫療器材製造廠和醫療機構採取措施，確保採取適當的防護措施，以減少由於網路攻擊而導致器材故障的風險。

附錄三：本產品相關之通用漏洞揭露 (Common Vulnerabilities and Exposures, CVE)

通用漏洞揭露(Common Vulnerabilities and Exposures, CVE)是資訊安全相關的資料庫，該資料庫收集各種資安漏洞並給予編號以便於查閱，讓資安管理人員有辦法針對部分CVE所條列的系統弱點逐項檢測。此資料庫現由美國非營利組織 MITRE所屬的National Cybersecurity FFRDC所營運維護。將所獲得資訊羅列。

用Watch(手錶)關鍵字所獲得的資料詳如表一。

表一、CVE資料庫(關鍵字:Watch)

漏洞編號	說明
CVE-2020-29484	An issue was discovered in Xen through 4.14.x. When a Xenstore watch fires, the xenstore client that registered the watch will receive a Xenstore message containing the path of the modified Xenstore entry that triggered the watch, and the tag that was specified when registering the watch. Any communication with xenstored is done via Xenstore messages, consisting of a message header and the payload. The payload length is limited to 4096 bytes. Any request to xenstored resulting in a response with a payload longer than 4096 bytes will result in an error. When registering a watch, the payload length limit applies to the combined length of the watched path and the specified tag. Because watches for a specific path are also triggered for all nodes below that path, the payload of a watch event message can be longer than the payload needed to register the watch. A malicious guest that registers a watch using a very large tag (i.e., with a registration operation payload length close to the 4096 byte limit) can cause the generation of watch events with a payload length larger than 4096 bytes, by writing to Xenstore entries below the watched path. This will result in an error condition in xenstored. This error can result in a NULL pointer dereference, leading to a crash of xenstored. A malicious guest administrator can cause xenstored to crash, leading to a denial of service. Following a xenstored crash, domains may continue to run, but management operations will be impossible. Only C xenstored is affected, oxenstored is not affected. **Published:** 12/15/2020
CVE-2018-7926	Huawei Watch 2 with versions and earlier than OWDD.180707.001.E1 have an improper authorization vulnerability. Due to improper permission configuration for specific operations, an attacker who obtained the Huawei ID bound to the watch can bypass permission verification to perform specific operations and modify some data on the watch. **Published**: 11/13/2018
CVE-2019-20470	An issue was discovered on TK-Star Q90 Junior GPS horloge 3.1042.9.8656 devices. It performs actions based on certain SMS

	commands. This can be used to set up a voice communication channel from the watch to any telephone number, initiated by sending a specific SMS and using the default password, e.g., pw,<password>,call,<mobile_number> triggers an outbound call from the watch. The password is sometimes available because of CVE-2019-20471. **Published:** 02/01/2021