醫療器材網路安全評估分析參考範本

「植入式心律器之脈搏產生器」

衛生福利部食品藥物管理署

110 年 12 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

植入式心律器之脈搏產生器

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

報告編號 (Report No.)	*CS-001*	報告版本 (Report Version)	B
公司名稱 (Company Name)	ABC醫材股份有限公司		
電話(TEL)	02-2XXXXXXX	傳真(FAX)	02-2XXXXXXX
製造業者地址 (Factory Address)	OO市OO區OO路		
審查者 (Review By)	報告製作者 (Prepared By)	評估日期 (Evaluation Period)	報告日期 (Report Date)
林OO	劉OO	110/11/XX	110/11/XX

目　錄

1. 簡介(Introduction)

1.1 報告概述(Document Overview)

本報告包括醫療器材「植入式心律器之脈搏產生器」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)

本報告之評估人員清單請參照下表1.2.1：

表1.2.1、網路安全分析評估人員清單

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
劉 OO	研發一部	高級軟體工程師	OO 大學資工系 碩士	OO 科技 系統工程師	ICCP 認證	10 年	產品安全評估
鐘 OO	資訊科技部門	網路工程師	OO 大學電機系 學士	OO 電子 通訊工程師	SSCP 認證	8 年	網路安全評估
林 OO	法務部門	法規專員	OO 大學法律系 學士	OO 科技 法規助理	OO 證照	7 年	醫療法規符合性評估

1.3 引用文件(Document References)

1.3.1 引用的專案文件(Project References)

本報告參照之技術文件如下表1.3.1.1：

表1.3.1.1、參照技術文件

序號 #	文件編號 Document Identifier	文件標題 Document Title
1		Software Requirements Specification

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

本報告參照之網路安全與風險分析相關法規如下表1.3.2.1：

表1.3.2.1、參照標準與法規

序號 #	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	

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

本公司之網路安全評估團隊，全系統面的分析植入式心律器之脈搏產生器之可能的網路安全風險認為：

- 網路安全的相關保護措施已經考量並於研發階段已經執行。
- 根據目前已執行的安全保護規範，其殘餘風險是可接受的，對於系統安全具有保障。
- 具有良好管道可以取得生產以及售後服務資訊，可進行產品品質控管

本植入式心律器之脈搏產生器產品經評估其剩餘網路安全風險，處於可接受的等級，其產品之效益遠大於風險危害，同意本產品之設計。

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)

植入式心臟裝置是為了恢復正常生理性心臟電傳導功能，其包含心臟節律器(Pacemaker)、植入式心律去顫器（Implantable Cardioverter Defibrillators, ICD）和心臟再同步去顫器（Cardiac Resynchronization Therapy Defibrillators, CRT-Ds）。

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所示：

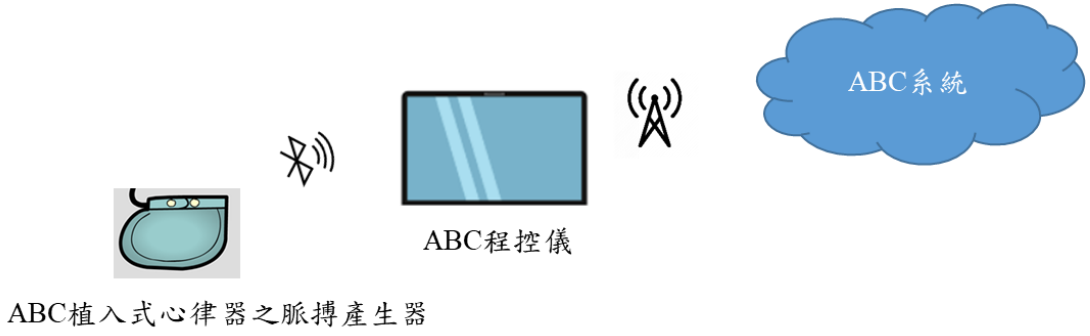


圖2.1.3.1、ABC植入式心律器之脈搏產生器系統架構圖

ABC 程控儀可透過無線藍牙(Bluetooth Specification v5.2)設定ABC 植入式心律器之脈搏產生器，ABC 程控儀可與 ABC 系統連結。若您透過 Wi-Fi 連接網路，建議使用安全的 Wi-Fi 網路(例如使用WPA3 或更新的網路安全協定)。ABC 系統允許查看、儲存或

檢索患者和脈搏產生器資料，ABC 公司對於個人資料之蒐集、處理和利用符合我國《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，使用者應遵守個人資料保護法之規範。本植入式心律器之脈搏產生器的操作與使用，主要功能分為設定及資料傳輸如下表2.1.3.1所示。

表2.1.3.1、植入式心律器之脈搏產生器應用情境

應用情境	說明	資產
設定植入式心律器之脈搏產生器	臨床醫師透過程控儀設定植入式心律器之脈搏產生器	韌體、作業系統、系統組態檔、通訊協定、資料
資料傳輸	使用者透過無線方式進行資料傳輸	通訊協定、機敏性資料

本植入式心律器之脈搏產生器設備運作時所需組成元素(資產)如下表2.1.3.2所示。

表2.1.3.2、植入式心律器之脈搏產生器設備資產清單

資產名稱	說明
作業系統	控制植入式心律器之脈搏產生器軟、硬體模組，包含或不包含檔案系統(File System)之核心軟體。
韌體	燒錄在植入式心律器之脈搏產生器電路板中儲存媒介(如 Flash 晶片)，對於植入式心律器之脈搏產生器正常運作必要之軟體。
系統組態檔	定義作業系統及軟體運作方式之重要設定檔，例如 IP 設定。
機敏性資料	使用者的帳號、病患資料等。
日誌資料	系統發生安全事件或是非授權使用者異常操作的紀錄資料檔。
通訊協定	裝置或系統間的通訊協定

本產品之軟體物料清單如下表2.1.3.3：

表2.1.3.3、植入式心律器之脈搏產生器軟體物料清單

名稱	來源	版本
GNU Compiler Collection (GCC)	GNU Project	GCC 10.2
Python 3	Python	Python 3.0

本產品中的資料受到密碼、加密以及系統內安全連接的保護。

- 密碼–所有帳戶都必須使用強化密碼。密碼建立規則用於確保您建立的密碼

難以讓別人猜中。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保密資訊，方法是除預定使用者之外的任何人均無法讀取資料 。
- 安全連接 – 資料傳輸僅透過與受信任的系統進行安全連接。網路埠(Network Ports): 本產品保留 TCP 埠（3001、3002、3010、3020、3021、3050、4001、5100、5101 和 10001）來識別程控儀的類型。

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

本產品之網路安全要求參考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	是	SRS-03
	使用該演算法支援的最大金鑰長度	是	SRS-04
	不使用自行創造的加密方式	是	SRS-05
	加密金鑰具有保護機制	是	SRS-06
	加密金鑰或憑證週期性更換	是	SRS-07
完整性	重要資料產生 HASH 值，確保其完整性	是	SRS-08
	重要資料傳輸過程，使用防止竄改的協定	是	SRS-09
	提供下載的資料，產生 HASH 值供比對其完整性	是	SRS-10
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-11

[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.

	驗證使用者輸入資料	是	SRS-12
	驗證外部取得的資料	不適用	
	驗證系統參數合理性	是	SRS-13
	於伺服器端檢查輸入資料合法性	是	SRS-14
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	是	SRS-15
	身分認證機制位於伺服端且採用集中管理機制	是	SRS-16
	採用多重因素認證(兩種以上認證類型)	是	SRS-17
	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	是	SRS-18
	身分認證相關資訊不存於源碼中，並限制存取	是	SRS-19
	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非公開功能	不適用	
	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	是	SRS-20
	執行功能或存取資源前，檢查使用者授權	是	SRS-21
	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	不適用	
	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-22
	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-23
	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	是	SRS-24
	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-25
	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-26
	作業平台定期更新、關閉不必要服務、注意安全設定	是	SRS-27
	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-28

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	資料傳輸的封包，送出前需要做加密
SRS-02	資料接收端儲存資料時會做加密處理
SRS-03	資料傳輸儲存使用的加密制度，為公開、國際機構驗證且未遭破解的演算法
SRS-04	資料傳輸儲存使用的加密制度演算法所支援最大金鑰長度，提高加密強度
SRS-05	資料傳輸儲存使用的加密方式為公開、國際機構驗證的加密制度
SRS-06	加密金鑰具有保護機制，以確保金鑰不會外洩
SRS-07	本產品會週期性的更換加密制度所使用的金鑰
SRS-08	對於重要資料會使用雜湊(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-09	資料傳輸過程會使用安全的協定，防止資料被竄改
SRS-10	對於重要資料接收端，會給予雜湊(HASH)值校驗，以保證檔案與資料確實是由原創者所提供
SRS-11	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
SRS-12	本產品會對使用者輸入之資料進行驗證
SRS-13	本產品對於產生之參數會判斷其合理性，例如:電擊設定是否異常
SRS-14	本產品會於伺服器端檢查使用者輸入之資料合法性
SRS-15	本產品除了允許匿名存取之功能，所有功能都須經過身分認證才可以允許存取
SRS-16	本產品之身分驗證會在伺服器端進行，接收到使用者身分資訊後會傳回伺服器端資料庫進行驗證
SRS-17	本產品之身分驗證採用多重認證
SRS-18	本產品之身分驗證過程中，使用者身分資訊不會明文傳輸
SRS-19	本產品之身分驗證資訊不會包含於程式源碼中，未經身分驗證會限制存取
SRS-20	本產品之授權與存取控制於伺服器端集中管理
SRS-21	本產品執行功能或進行資料存取前，會檢查使用者是否經過伺服器的授權
SRS-22	本產品使用者之執行權限皆為最小的執行權限
SRS-23	在使用者認證失敗、或存取失敗、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 紀錄存放於伺服器端
SRS-24	本產品在使用者進行會話功能時產生的會話識別碼是隨機產生的
SRS-25	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-26	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-27	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-28	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	將資料做傳輸前，需要做AES128 的加密
SDD-02	資料儲存時，需做AES128加密進行儲存
SDD-03	資料傳輸儲存使用的加密制度為進階加密標準(AES)
SDD-04	資料傳輸儲存使用的進階加密標準所使用的最大金鑰長度為128位元，確保金鑰的保密
SDD-05	資料傳輸儲存使用的密碼會週期性更換
SDD-06	重要資料在傳輸時使用雜湊(HASH)作為檔案校驗碼
SDD-07	資料傳輸過程會使用安全通訊加密的協定(SSL)
SDD-08	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-09	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-10	輸入驗證會於伺服器端檢查輸入資料是否符合
SDD-11	啟用產品功能前須先經過伺服器之身分認證
SDD-12	身分驗證會使用藍芽UUID進行驗證
SDD-13	本產品對使用者僅開放最小使用權限
SDD-14	於伺服器端會有一Log記錄所有對於本系統進行之認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者等行為
SDD-15	使用者進行app連線會話時，會產生隨機的會話識別碼(Session ID)
SDD-16	產品發生錯誤時，系統會將資源釋放，回復尚未輸入的狀態
SDD-17	針對系統使用的外部軟體或元件會更改其預設密碼，定期注意其安全漏洞報告並更新
SDD-18	設定權限管理
SDD-19	針對特權帳戶定期盤點
SDD-20	權限管理
SDD-21	軟體的完整性保護
SDD-22	自動化組態設定
SDD-23	建置區塊鏈保護機制

SDD-24	自動登出，以防止器材遭受未經授權人員存取。
SDD-25	使用帳號與密碼才能設定系統。
SDD-26	設備身分管理機制

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

表2.4.1到表2.4.11為植入式心律器之脈搏產生器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1

測試編號	SVV-01
軟體版本	1.3.4
測試項目	傳輸封包做AES128加密
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	封包可以用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	1.3.4
測試項目	資料儲存時，需做AES128加密進行儲存
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	ABC線上管理系統中的資料使用AES128加密儲存
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	1.3.4
測試項目	金鑰測試
測試人員	王小民

測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	**1.** 輸入超過最大長度解密失敗，範圍內長度解密成功 **2.** 金鑰定期更換
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	1.3.4
測試項目	使用雜湊為重要檔案進行校驗
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	接收檔案後，進行雜湊校驗，以保證檔案與資料確實是由原創者所提供
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	1.3.4
測試項目	輸入驗證
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	**1.** 會過濾使用者輸入的惡意命令或資料 **2.** 輸入正確資訊，回傳伺服器，伺服器能正確接收資訊
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	1.3.4
測試項目	身分驗證
測試人員	王小民

測試日期	2020/10/1
測試方法依據	ABC Test Protool (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	**1.** 進行功能前需先經過身分驗證 **2.** 輸入正確身分資訊，會與伺服器資訊進行比對且正確
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	1.3.4
測試項目	授權與存取控制
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	**1.** 使用者未經過授權無法使用系統功能 **2.** 獲得授權之使用者僅有最小權限
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	1.3.4
測試項目	日誌記錄
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	系統進行的所有行為都會進行Log之紀錄
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	1.3.4
測試項目	會話管理
測試人員	王小民

測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	使用者進行app連線會話時，會產生隨機會話識別碼(Session ID)
測試結果	Pass

表2.4.10、網路安全驗證確效測試10

測試編號	SVV-10
軟體版本	1.3.4
測試項目	錯誤及例外管理
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	出現錯誤時，系統成功將資源釋放，回復尚未輸入的狀態
測試結果	Pass

表2.4.11、網路安全驗證確效測試11

測試編號	SVV-11
軟體版本	1.3.4
測試項目	外部元件、軟體之預設密碼
測試人員	王小民
測試日期	2020/10/1
測試方法依據	ABC Test Protocol (Doc. No.:ABC-100-002, Rev.1)
測試通過標準	使用外部元件或軟體時輸入預設密碼時，無法正確使用
測試結果	Pass

2.5 追溯性矩陣(Traceability Matrix)

表2.5.1為植入式心律器之脈搏產生器追溯性矩陣。

表2.5.1 系統追溯性矩陣

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-03	SVV-01

SRS-04	SDD-04	SVV-03
SRS-05	SDD-03	SVV-03
SRS-06	SDD-05	SVV-03
SRS-07	SDD-06	SVV-03
SRS-08	SDD-07	SVV-04
SRS-09	SDD-08	SVV-04
SRS-10	SDD-07	SVV-04
SRS-11	SDD-09	SVV-05
SRS-12	SDD-10	SVV-05
SRS-13	SDD-10	SVV-05
SRS-14	SDD-10	SVV-05
SRS-15	SDD-11	SVV-06
SRS-16	SDD-12	SVV-06
SRS-17	SDD-12	SVV-06
SRS-18	SDD-12	SVV-06
SRS-19	SDD-12	SVV-06
SRS-20	SDD-13	SVV-07
SRS-21	SDD-13	SVV-07
SRS-22	SDD-13	SVV-07
SRS-23	SDD-14	SVV-08
SRS-24	SDD-15	SVV-09
SRS-25	SDD-16	SVV-10
SRS-26	SDD-17	SVV-11
SRS-27	SDD-17	SVV-11
SRS-28	SDD-17	SVV-11

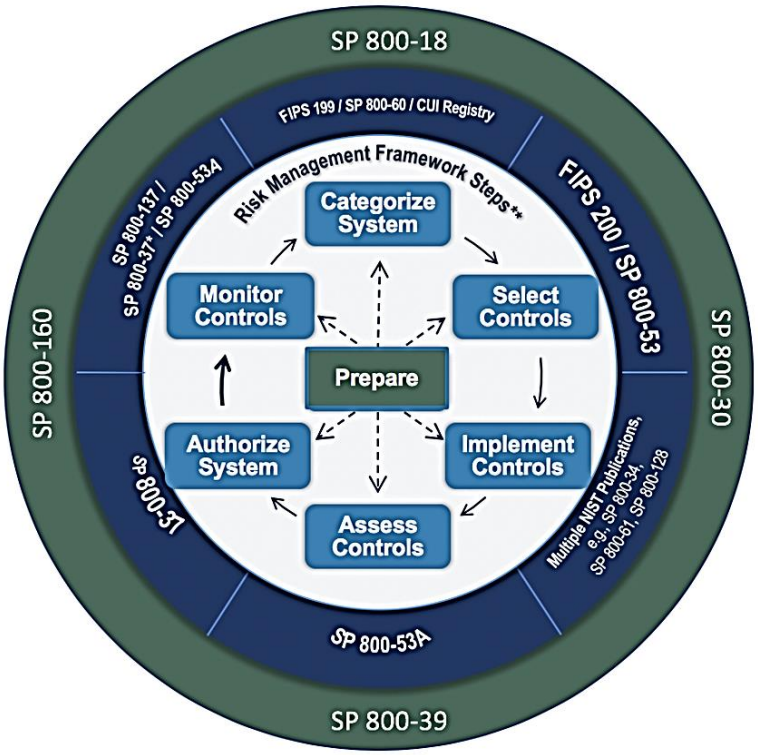
3. 網路安全評估(Cybersecurity Assessment)

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 模型的威脅。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)

表3.1.2.1針對系統的資產識別，將系統資產加以分類。

表3.1.2.1、識別資產分類描述

資產名稱	資產項目
作業系統	控制植入式心律器之脈搏產生器軟、硬體模組 檔案系統(File System)之核心軟體
韌體	儲存媒介(如Flash 晶片)資料之存取

	植入式心律器之脈搏產生器之流程控制軟體
系統組態檔	作業系統設定檔案 軟體重要設定檔
機敏性資料	使用者的帳號 使用者使用資料
日誌資料	系統發生安全事件紀錄資料檔 非授權使用者異常操作紀錄資料檔
通訊協定	wifi通訊協定資料傳送 藍芽通訊協定資料傳送

3.2 資料流向圖(Data Flow Diagram, DFD)

本產品使用案例如下圖3.2.1所示：

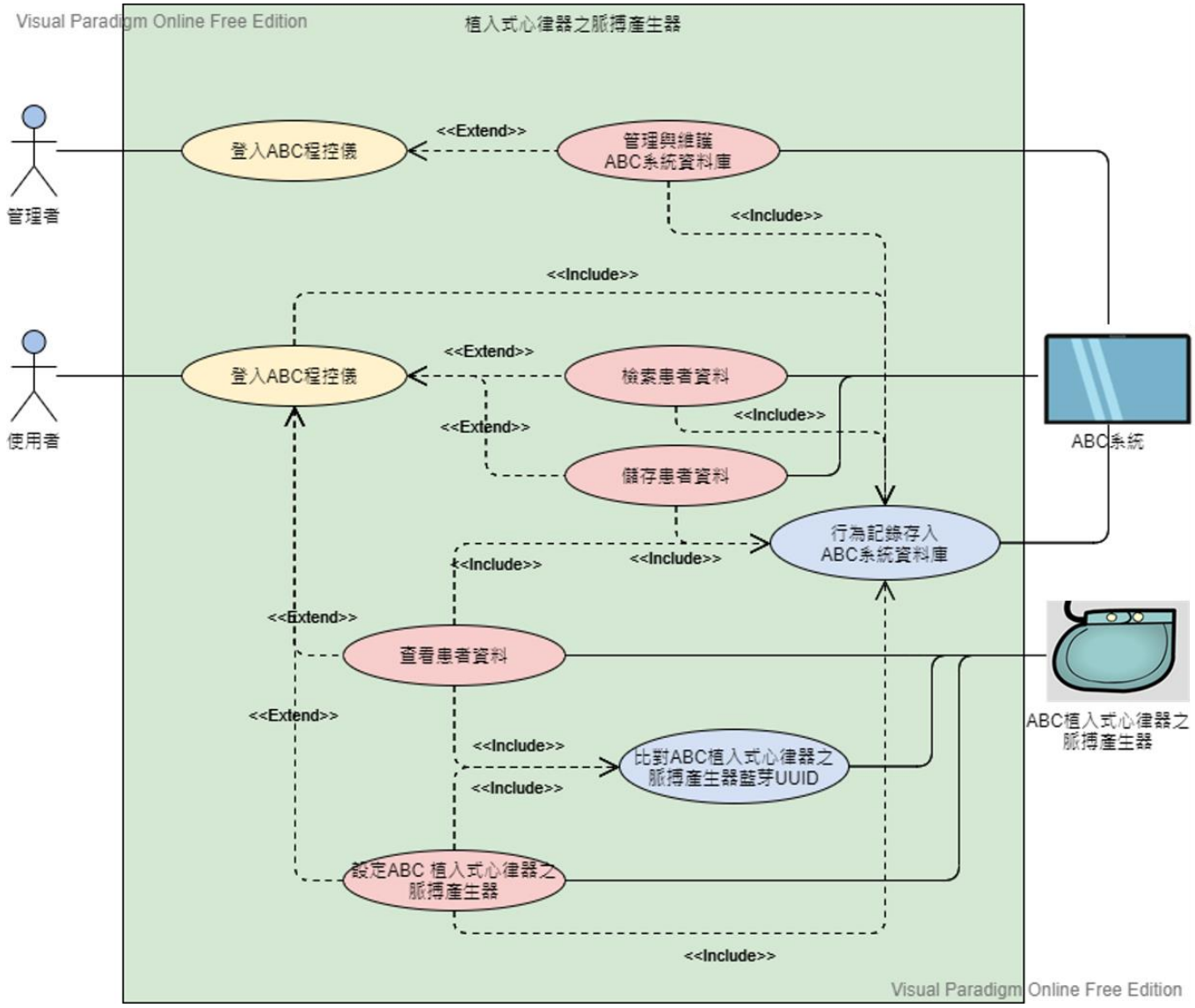


圖3.2.1、ABC植入式心律器之脈搏產生器使用案例圖

以資料角度描述系統元素如下：

- 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。

本系統之資料流向圖，如下圖3.2.2所示：

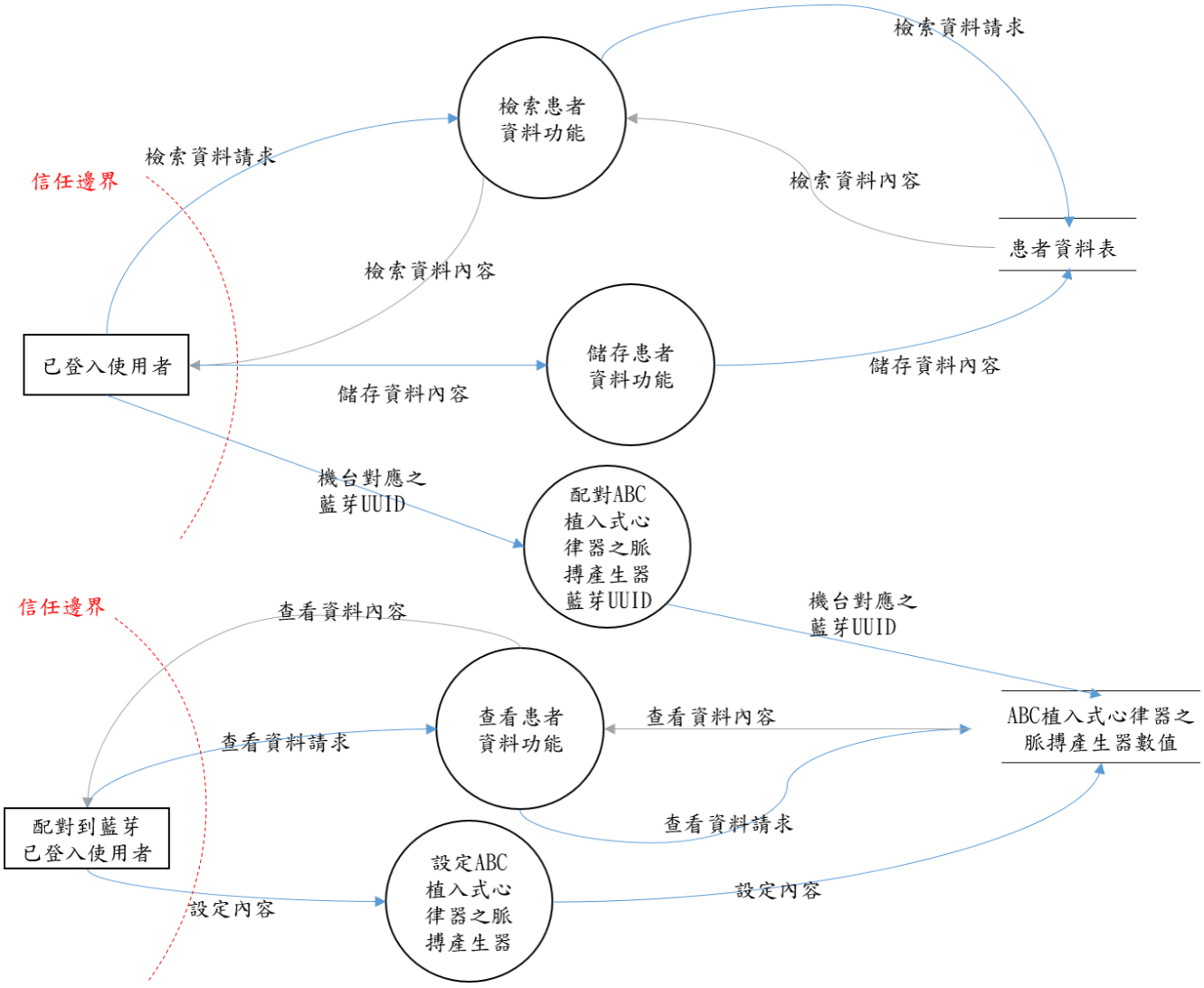


圖3.2.2、ABC植入式心律器之脈搏產生器資料流向圖

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

表3.3.1為依據STRIDE模型威脅分類以及風險降低措施來建立的網路安全威脅分析表。

表3.3.1、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	V	D1：透過入侵作業系統關閉相關服務或應用系統 E1：作業系統遭到入侵後，可透過創建帳號並提權。
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。患者的植入式心律器之脈搏產生器之設定遭受未經授權的變更。植入式心律器之脈搏產生器無法正常運作，對患者造成傷害。
機敏性資料							I2：針對未保護的機敏性資料進行揭露
日誌資料		V	V				T3：竄改日誌資料，隱匿不法行為 R1：竄改日誌資料，修改相關存取記錄
通訊協定	V						S1：透過重送攻擊來進行假冒攻擊 I3：針對未保護的通訊管道揭露資訊

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：

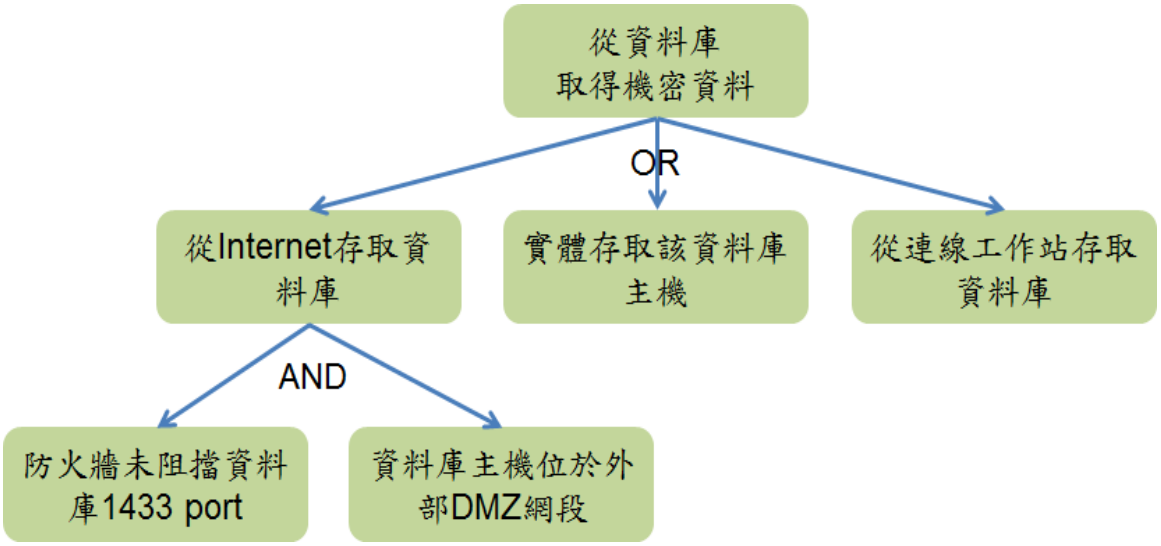


圖3.3.1、攻擊樹狀圖

本系統之威脅模型圖(Threat Model Diagram)，如下圖3.3.2所示：

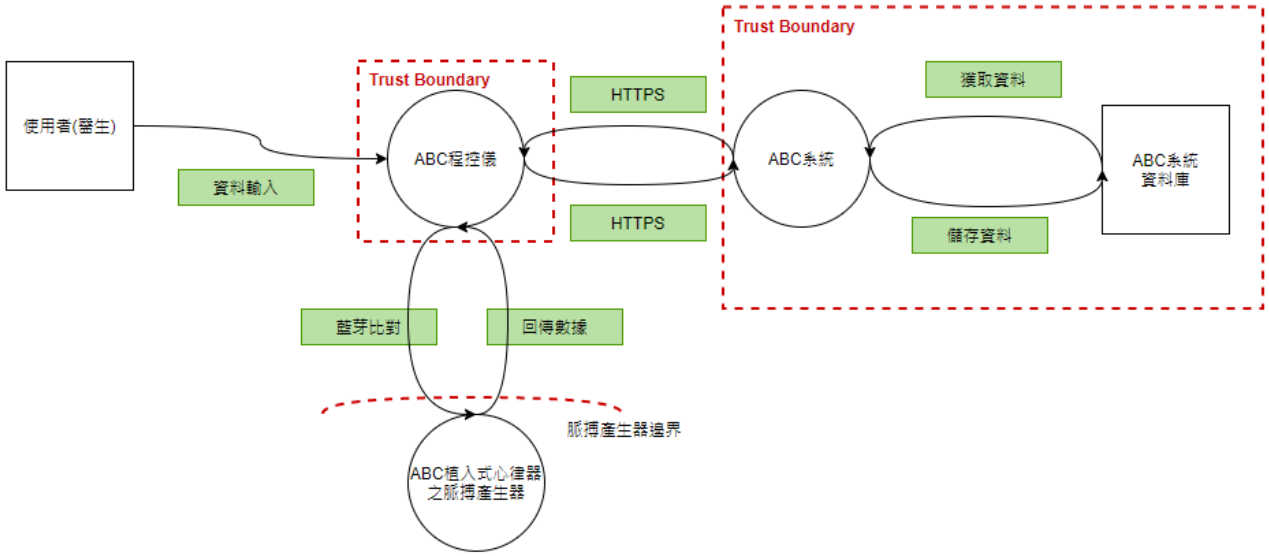


圖3.3.2、ABC植入式心律器之脈搏產生器威脅模型

3.4 網路安全風險評鑑方法(Cybersecurity Risk Assessment Methodology)[3][4][5]

關於本產品之網路安全風險等級請參考下表3.4.1。

表3.4.1、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	2	2	1	2	2	1	1.66	1	1.66	低風險 (可接受)	Risk-01	SDD-18：設定權限管理
作業系統	E1	1	2	1	2	2	2	1	1.66	1	1.66	低風險 (可接受)	Risk-02	SDD-19：針對特權帳戶定期盤點 SDD-20：權限

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

[4] 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

[5]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

														管理
韌體	T1	1	2	1	1	1	2	1	1.33	1	1.33	低風險 (可接受)	Risk-03	SDD-21：軟體的完整性保護
韌體	I1	1	1	2	1	2	2	1	1.5	1	1.5	低風險 (可接受)	Risk-04	SDD-01：進將資料做傳輸前，需要做AES128的加密。 SDD-02: 資料儲存時，需做AES128加密進行儲存
系統組態檔	T2	1	1	2	3	2	1	1	1.66	1	1.66	低風險 (可接受)	Risk-05	SDD-22：自動化組態設定
系統組態檔	D2	1	2	1	1	2	2	1	1.5	1	1.5	低風險 (可接受)	Risk-06	SDD-22：自動化組態設定
機敏性資料	I2	2	1	1	1	1	1	1	1	1	2	低風險 (可接受)	Risk-07	SDD-01：進將資料做傳輸前，需要做AES128的加密。 SDD-02: 資料儲存時，需做AES128加密進行儲存

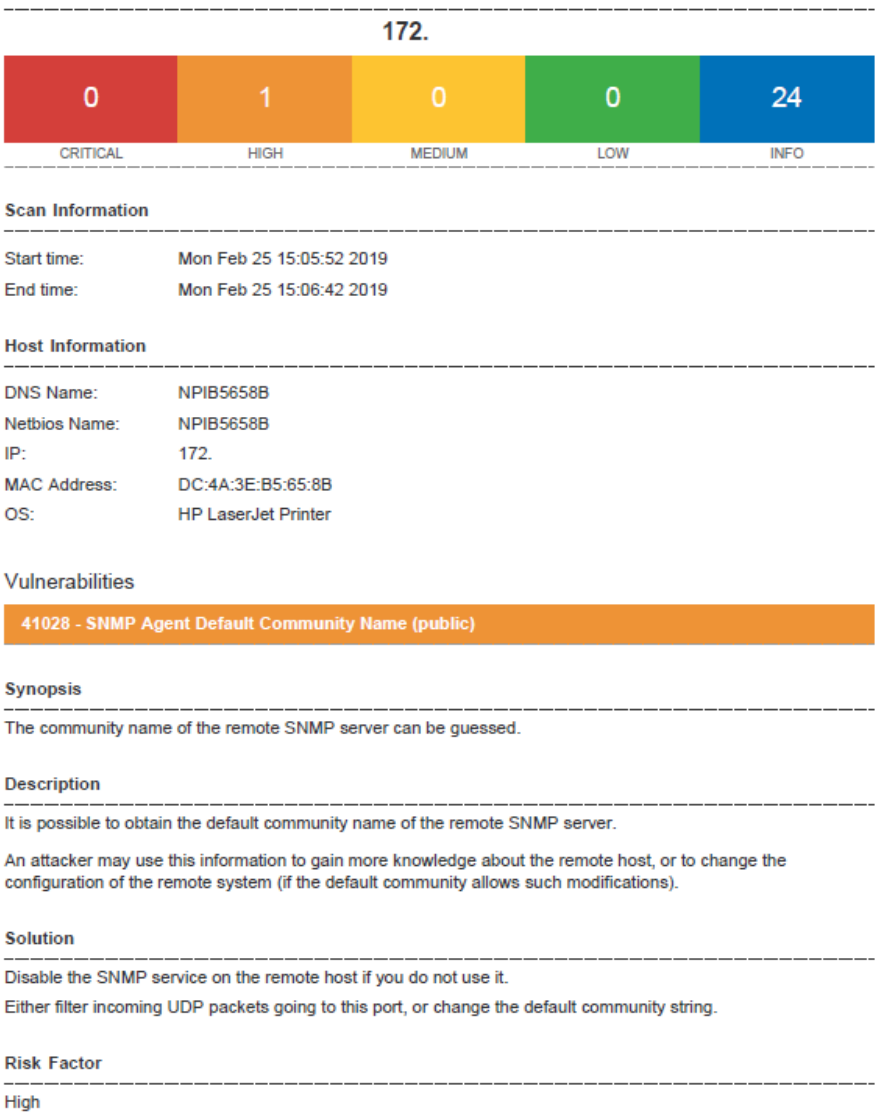
日誌資料	T3	1	2	1	3	1	2	1	1.66	1	1.66	低風險 (可接受)	Risk-08	SDD-23：建置區塊鏈保護機制
日誌資料	R1	1	1	1	1	1	1	1	1	1	1	低風險 (可接受)	Risk-09	SDD-24：自動登出，以防止器材遭受未經授權人員存取。 SDD -25：使用帳號與密碼才能設定植入式心律器之脈搏產生器。
通訊協定	S1	1	1	1	1	1	2	1	1.16	1	1.16	低風險 (可接受)	Risk-10	SDD -26：設備身分管理機制
通訊協定	I3	1	2	1	1	1	2	1	1.33	1	1.33	低風險 (可接受)	Risk-11	SDD-01：進將資料做傳輸前，需要做AES128的加密。 SDD-02: 資料儲存時，需做AES128加密進行儲存

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[67]。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。

漏洞掃描測試報告如下圖3.5.1.1所示：



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

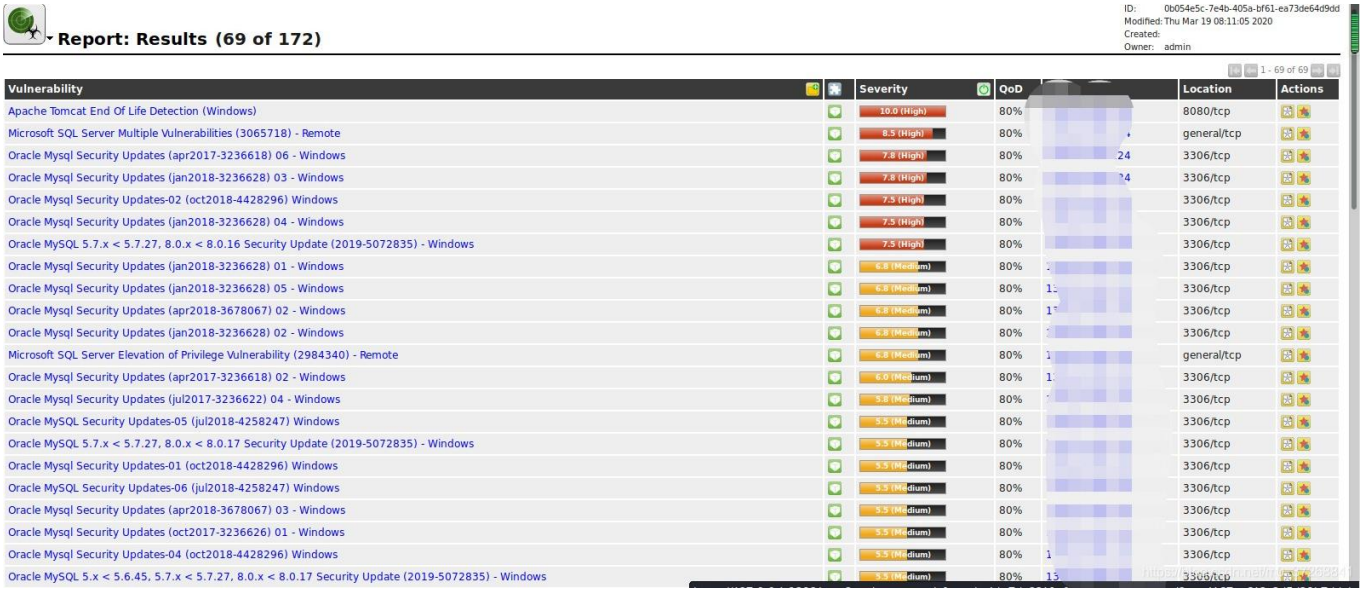
圖3.5.1.1、漏洞掃描測試報告圖

[6] Microsoft 威脅模型化工具. Available: https://docs.microsoft.com/zh-tw/azure/security/develop/threat-modeling-tool-threats
[7] 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

3.5.2 滲透測試(Penetration Testing)

滲透測試(Penetration Test)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。

滲透測試報告如下圖3.5.2.1所示：



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、滲透測試報告圖

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

詳見附件“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)

本章節彙整 2013~2020 年間美國FDA 網路安全通知(詳如表1)，在 2017~2019 年間有多起的植入式心律器之脈搏產生器相關網路安全通知，如附錄二表1所示。

附錄二表1、美國FDA 網路安全通知彙整(2013~2020 年)[8][9]

日期	安全通知
2020/03/03	SweynTooth 網路安全漏洞可能會影響某些醫療器材
2020/01/23	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
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
2019/03/21	影響Medtronic 植入式心臟器材、程控儀(Programmers)和家用監測器的網路安全漏洞
2018/10/11	網路安全更新影響Medtronic 植入式心臟器材程控儀
2018/04/17	某些雅培(Abbott)(以前為St. Jude Medical)植入心臟器材的電池性能警報和網路安全韌體更新
2017/8/29	韌體更新以解決在雅培(以前為St. Jude Medical) 植入式心律調節器中發現的網路安全漏洞
2017/01/09	在 St.Jude Medical 的植入式心臟器材和Merlin @ home Transmitter 中發現了網路安全漏洞
2013/6/13	醫療器材和醫院網路的網路安全

依據 2019 年 3 月 21 日的網路安全通知，某些美敦力產品含有潛在的網路安全漏洞[10]。這些漏洞發生於使用Conexus 無線射頻通訊技術的產品。Conexus 具有網路安全漏洞是因為它不使用加密，受影響產品之網路漏洞可能使未經授權的人能夠讀取並可能改變植入式心臟電子儀器、監測器或程控儀的設定。

[8] https://www.fda.gov/medical-devices/digital-health/cybersecurity#safety
[9] https://www.accessdata.fda.gov/cdrh_docs/pdf/P980016S436M.pdf
[10] https://consumer.fda.gov.tw/Light/newsDetail.aspx?nodeID=217&id=4194

附錄二圖1、Medtronic MyCareLink™ Patient Monitor

Conexus 無線射頻通訊技術被用來實現設備之間的通訊，並允許Medtronic 程控儀和監測器執行以下一項或多項操作，如上附錄二圖2所示：

- 將患者體內植入的心臟設備之資料遠程傳輸到指定的醫療診所（遠程監控），包括重要的操作和安全通知；
- 允許臨床醫生即時顯示和列印設備資訊；
- 允許臨床醫生設定植入設備。

使用者應遵循下列指導原則， 以降低這些漏洞的風險：

- 僅使用自醫療院所或美敦力公司直接取得的遠端監測器以確保系統的完整性。
- 遠端監測器必須保持在開機狀態，以確保由醫師設定的無線

  CareAlerts 和自動安排的遠程傳輸如期發生。
- 妥善管控遠端監測器實體。
- 向醫療院所或美敦力公司回報有關這些產品的疑慮。

美敦力（Medtronic）的植入式心律去顫器（Implantable Cardioverter Defibrillators, ICD）和心臟再同步去顫器 （Cardiac Resynchronization Therapy Defibrillators, CRT-Ds）受影響的型號如下:

- Amplia MRI CRT-D, all models
- Claria MRI CRT-D, all models
- Compia MRI CRT-D, all models

- Concerto CRT-D, all models
- Concerto II CRT-D, all models
- Consulta CRT-D, all models
- Evera MRI ICD, all models
- Evera ICD, all models
- Maximo II CRT-D and ICD, all models
- Mirro MRI ICD, all models
- Nayamed ND ICD, all models
- Primo MRI ICD, all models
- Protecta CRT-D and ICD, all models
- Secura ICD, all models
- Virtuoso ICD, all models
- Virtuoso II ICD, all models
- Visia AF MRI ICD, all models
- Visia AF ICD, all models
- Viva CRT-D, all models

受影響的程控儀(Programmers)和家用監測器如下:

- CareLink 2090 Programmer
- MyCareLink Monitor, models 24950 and 24952
- CareLink Monitor, Model 2490C

MyCareLink 家用監測器（24950 和 24952 型）用無線技術連接到患者的植入式心臟器材並讀取該器材上所儲存的資料。位於患者家中的發送器使用家用電話、行動電話或無線網路（wi-fi）通過 CareLink Network 將患者的資料發送給他的醫生。

附錄二表2呈現美敦力之MyCareLink 24950 於美國國家漏洞資料庫的資訊，以CVE-2019-6540 為例呈現評估。

附錄二表2、MyCareLink 24950 於美國國家漏洞資料庫的資訊

漏洞編號	說明
CVE-2019-6540	The Conexus telemetry protocol utilized within Medtronic MyCareLink Monitor versions 24950 and 24952, CareLink Monitor version 2490C, CareLink 2090 Programmer, Amplia CRT-D, Claria CRT-D, Compia CRT-D, Concerto CRT- D, Concerto II CRT-D, Consulta CRT-D, Evera ICD, Maximo II CRT-D and ICD, Mirro ICD, Nayamed ND ICD, Primo ICD, Protecta ICD and CRT-D, Secura

	ICD, Virtuoso ICD, Virtuoso II ICD, Visia AF ICD, and Viva CRT-D does not implement encryption. An attacker with adjacent short-range access to a target product can listen to communications, including the transmission of sensitive data. Published: 三月 26, 2019; 2:29:01 下午 V3.0:6.5 MEDIUM V2.0:3.3 LOW
CVE-2019-6538	The Conexus telemetry protocol utilized within Medtronic MyCareLink Monitor versions 24950 and 24952, CareLink Monitor version 2490C, CareLink 2090 Programmer, Amplia CRT-D, Claria CRT-D, Compia CRT-D, Concerto CRT-D, Concerto II CRT-D, Consulta CRT-D, Evera ICD, Maximo II CRT-D and ICD, Mirro ICD, Nayamed ND ICD, PrimoICD, Protecta ICD and CRT-D, Secura ICD, Virtuoso ICD, Virtuoso II ICD, Visia AF ICD, and Viva CRT-D does not implement authentication or authorization. An attacker with adjacent short-range access to an affected product, in situations where the product's radio is turned on, can inject, replay, modify, and/or intercept data within the telemetry communication. This communication protocol provides the ability to read and write memory values to affected implanted cardiac devices; therefore, an attacker could exploit this communication protocol to change memory in the implanted cardiac device. Published: 三月 25, 2019; 6:29:00 下午-0400 V3.0:6.5 MEDIUM V2.0:3.3 LOW
CVE-2018-10626	A vulnerability was discovered in all versions of Medtronic MyCareLink 24950 and 24952 Patient Monitor. The affected product's update service does notsufficiently verify the *authenticity* of the data uploaded. An attacker who obtains per-product credentials from the monitor and paired implantable cardiac device information can potentially upload invalid data to the Medtronic CareLink network. **Published:** 八月 10, 2018; 2:29:00 下午 -0400 V3.0:4.4 MEDIUM V2.0:3.8 LOW
CVE-2018-10622	A vulnerability was discovered in all versions of Medtronic MyCareLink 24950 and 24952 Patient Monitor. The affected products use per-productcredentials that are stored in a recoverable format. An attacker can use these credentials for network authentication and encryption of local data at rest. **Published:** 八月 10, 2018; 2:29:00 下午 -0400 V3.0:7.1 HIGH

	V2.0:1.9 LOW
CVE-2018-8870	Medtronic MyCareLink Patient Monitor, 24950 MyCareLink Monitor, all versions, and 24952 MyCareLink Monitor, all versions contains a hard-coded operating system password. An attacker with physical access can remove the case of the device, connect to the debug port, and use the password to gain privileged access to the operating system. Published: 七月 02, 2018; 9:29:01 下午 -0400 V3.0:6.8 MEDIUM V2.0:7.2 HIGH
CVE-2018-8868	Medtronic MyCareLink Patient Monitor,24950 *MyCareLink* Monitor, all versions,and 24952 MyCareLink Monitor, all versions, contains debug code meant to test the functionality of the monitor's communication interfaces, including the interface between the monitor and implantable cardiac device. An attacker with physical access to the device can apply the other vulnerabilities within this advisory to access this debug functionality. This debug functionality provides the ability to read and write arbitrary memory values to implantable cardiac devices via inductive or short range wireless protocols. An attacker with close physical proximity to a target implantable cardiac device can use this debug functionality. **Published:** 七月 02, 2018; 9:29:01 下午 -0400 V3.0:6.4 MEDIUM V2.0:6.9 MEDIUM

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)[11]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。用Pacemaker (心臟節律器)、Implantable Cardioverter Defibrillator（植入式心律去顫器）和Cardiac Resynchronization Therapy Defibrillator（心臟再同步去顫器）等關鍵字搜尋所獲得的資訊詳如附錄三表1～附錄三表3。

附錄三表1、CVE 資料庫(關鍵字: Pacemaker，僅列出部分資訊)

漏洞編號	說明
CVE-2017-12714	Abbott Laboratories pacemakers manufactured prior to Aug 28, 2017 do not restrict or limit the number of correctly formatted "RF wake-up" commands that can be received, which may allow a nearby attacker to repeatedly send commands to reducepacemaker battery life. CVSS v3 base score: 5.3, CVSS vector string: AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H. Abbott has developed a firmware update to help mitigate the identified vulnerabilities.
CVE-2017-12712	The authentication algorithm in Abbott Laboratories pacemakers manufactured prior to Aug 28, 2017, which involves an authentication key and time stamp, can be compromised or bypassed, which may allow a nearby attacker to issue unauthorized commands to the pacemaker via RF communications. CVSS v3 base score: 7.5, CVSS vector string: AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H. Abbott has developed a firmware update to help mitigate the identified vulnerabilities.

附錄三表2、CVE 資料庫(關鍵字: Implantable Cardioverter Defibrillator)

漏洞編號	說明
CVE-2018-8868	Medtronic MyCareLink Patient Monitor, 24950 MyCareLink Monitor, all versions, and 24952 MyCareLink Monitor, all versions, contains debug code meant to test the functionality of the monitor's communication interfaces, including the interfacebetween the monitor and implantable cardiac device. An attacker with physical access to the device can apply the other vulnerabilities within this advisory to access this debug functionality. This debug functionality provides the ability to read and write arbitrary memory values to implantable cardiac devices via inductive or short range wireless protocols. An attacker with close physical proximity to a target implantable cardiac device can use this debug functionality.
CVE-2018-10626	A vulnerability was discovered in all versions of Medtronic MyCareLink 24950 and 24952 Patient Monitor. The affected product's update service does not sufficiently verify the authenticity of the data uploaded. An attacker who obtains per-product credentials from the

[11] https://cve.mitre.org/

	monitor and paired implantable cardiac device information can potentially upload invalid datato the Medtronic CareLink network.
CVE-2013-7395	ZOLL Defibrillator / Monitor X Series has a default (1) supervisor password and (2) service password, which allows physically proximate attackers to modify device configuration and cause a denial of service (adverse human health effects).
CVE-2007-6756	ZOLL Defibrillator / Monitor M Series, E Series, and R Series have a default password for System Configuration mode, which allows physically proximate attackers to modify device configuration and cause a denial of service (adverse humanhealth effects).

附錄三表3、CVE 資料庫(關鍵字: Cardiac Resynchronization TherapyDefibrillator)

漏洞編號	說明
CVE-2019-6538	The Conexus telemetry protocol utilized within Medtronic MyCareLink Monitor versions 24950 and 24952, CareLink Monitor version 2490C, CareLink 2090 Programmer, Amplia CRT-D, Claria CRT-D, Compia CRT-D, Concerto CRT-D, Concerto II CRT-D, Consulta CRT-D, Evera ICD, Maximo II CRT-D and ICD, Mirro ICD, Nayamed ND ICD, Primo ICD, Protecta ICD and CRT-D, Secura ICD, Virtuoso ICD, VirtuosoII ICD, Visia AF ICD, and Viva CRT-D does not implement authentication or authorization. An attacker with adjacent short-range access to an affected product, in situations where the product’s radio is turned on, can inject, replay, modify, and/or intercept data within the telemetry communication. This communication protocol provides the ability to read and write memory values to affected implanted cardiac devices; therefore, an attacker could exploit this communication protocol to change memory in the implanted cardiac device.
CVE-2019-18254	BIOTRONIK CardioMessenger II, The affected products do not encrypt sensitive information while at rest. An attacker withphysical access to the CardioMessenger can disclose medical measurement data and the serial number from the implanted cardiac device the CardioMessenger is paired with.
CVE-2018-8868	Medtronic MyCareLink Patient Monitor, 24950 MyCareLink Monitor, all versions, and 24952 MyCareLink Monitor, all versions, contains debug code meant to test the functionality of the monitor's communication interfaces, including the interfacebetween the monitor and implantable cardiac device. An attacker with physical access to the device can apply the other vulnerabilities within this advisory to access this debug functionality. This debug functionality provides the ability to read and write arbitrary memory values to implantable cardiac devices via inductive or short range wireless protocols. An attacker with close physical proximity to a target implantable cardiac device can use this debug functionality.
CVE-2018-5552	Versions of DocuTrac QuicDoc and Office Therapy that ship with DTISQLInstaller.exe version 1.6.4.0 and prior contains ahard-coded cryptographic salt, "S@l+&pepper".

CVE-2018-5551	Versions of DocuTrac QuicDoc and Office Therapy that ship with DTISQLInstaller.exe version 1.6.4.0 and prior contain three credentials with known passwords: QDMaster, OTMaster, and sa.
CVE-2018-10626	A vulnerability was discovered in all versions of Medtronic MyCareLink 24950 and 24952 Patient Monitor. The affected product's update service does not sufficiently verify the authenticity of the data uploaded. An attacker who obtains per-product credentials from the monitor and paired implantable cardiac device information can potentially upload invalid data to the Medtronic CareLink network.
CVE-2017-13993	An Uncontrolled Search Path or Element issue was discoveredin i-SENS SmartLog Diabetes Management Software, Version 2.4.0 and prior versions. An uncontrolled search path element vulnerability has been identified which could be exploited by placing a specially crafted DLL file in the search path. If the malicious DLL is loaded prior to the valid DLL, an attacker could execute arbitrary code on the system. This vulnerability does not affect the connected blood glucose monitor and would not impact delivery of therapy to the patient.
CVE-2013-7395	ZOLL Defibrillator / Monitor X Series has a default (1) supervisor password and (2) service password, which allows physically proximate attackers to modify device configuration and cause a denial of service (adverse human health effects).
CVE-2007-6756	ZOLL Defibrillator / Monitor M Series, E Series, and R Series have a default password for System Configuration mode, which allows physically proximate attackers to modify device configuration and cause a denial of service (adverse human health effects).