醫療器材網路安全評估分析參考範本

「葡萄糖試驗系統」

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

葡萄糖試驗系統

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

報告編號 (Report No.)	*CS-002*	報告版本 (Report Version)	C
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)
李OO	吳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「葡萄糖試驗系統」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 **ABC** device, designed in **ABC** 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
吳 OO	軟體開發部	軟體工程師	OO 大學資工系 碩士	OO 軟體 研發工程師	OO 軟體領域	7 年	軟體程式之設計、測試及修正
謝 OO	硬體開發部	硬體工程師	OO 大學電機系 學士	OO 科技 研發工程師	OO 硬體領域	6 年	硬體線路設計、開發、除錯及改良 performance 及測試
李 OO	系統驗收部	測試工程師	OO 大學資工系 碩士	OO 科技 系統分析師	OO 認證	9 年	產品系統驗收測試

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，全系統面的分析葡萄糖試驗系統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

本葡萄糖試驗系統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)

應用程式須配合ABC血糖試紙設計為與ABC血糖機使用，適用於定量檢測採自指 尖、手掌、前臂和上臂的新鮮微血管全血的血糖，可幫助有效進行血糖監控。 ABC血糖試紙與ABC血糖機合用，適用於糖尿病患者的自我體外診斷檢測，同時透過藍芽將血糖資訊傳輸至ABC應用程式與管理軟體並上傳至ABC線上糖尿病管理系統，幫助專業醫護人員在臨床診療環境下的體外診斷檢測。

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葡萄糖試驗系統架構圖

ABC線上糖尿病管理系統讓患者檢視血糖資料。相容的ABC血糖機將資料透過無線

藍牙(Bluetooth Specification v5.2)傳輸到 ABC 糖尿病管理應用程式/軟體，該應用程式/軟體將資料上傳到ABC 線上糖尿病管理系統。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線上糖尿病管理系統的操作與使用，主要功能分為資料檢視及資料傳輸如下表2.1.3.1所示。

表2.1.3.1、ABC 線上糖尿病管理系統應用情境

應用情境	說明	資產
資料檢視	使用者檢視其資料	系統組態檔、通訊協定、應用服務、日誌資料、病患資料
資料傳輸	使用者透過網路進行資料傳輸	應用服務、通訊協定、病患資料

ABC 線上糖尿病管理系統設備運作時所需組成元素(資產)，如表2.1.3.2。

表2.1.3.2、ABC 線上糖尿病管理系統設備資產清單

	資產名稱
1.	作業系統
2.	系統組態檔
3.	應用服務
4.	日誌資料
5.	通訊協定
6.	病患資料

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。ABC線上糖尿病管理系統之系統要求如下表2.1.3.3所示：

表2.1.3.3、系統要求

類別	要求
支援的作業系統	● Microsoft Windows 10（32 位元/64 位元） ● Android 11
瀏覽器 (系統設計用於在受支援瀏覽器的 32 位元版本上操作。 系統還需要啟用 JavaScript 和 Cookies 以便順利執行。)	● 適用於 Windows 的 Microsoft Internet Explorer 11 ● 適用於 Windows 的 Chrome 86 ● 適用於 Android 的 Chrome 86

螢幕解析度	1024 x 768（建議的桌上型電腦最小像素尺寸） 320（建議的行動裝置最小像素寬度）

本產品之軟體物料清單如下表2.1.3.4：

表2.1.3.4、線上糖尿病管理系統軟體物料清單

名稱	來源	版本
Kotlin	JetBrains	Kotlin 1.3.72
OpenSSL	The OpenSSL Project	1.1.1h
HTTPd	Apache	2.4.46

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。

若您的網路使用防火牆，請注意允許應用程式在埠 80 和 443 上的出站連接到下列服務器的權限: abc.diabetes.com

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

[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.

	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
	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	不適用	

	(HASH)處理，才加以儲存		
	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用過濾機制，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:血糖值是否異常

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

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為葡萄糖試驗系統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 Protool (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 Protool (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 Protool (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 Protool (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 Protool (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 Protool (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 Protool (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 Protool (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 Protool (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）

下表2.5.1為葡萄糖試驗系統追溯性矩陣。

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

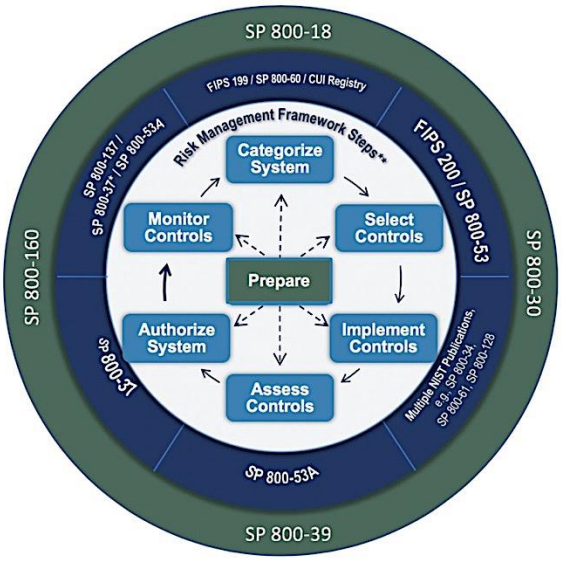
3. 本產品網路安全評估(Cybersecurity Assessment)

3.1 本產品網路安全評估計畫(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	控制葡萄糖試紙系統軟、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 葡萄糖試紙系統之流程控制軟體
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：

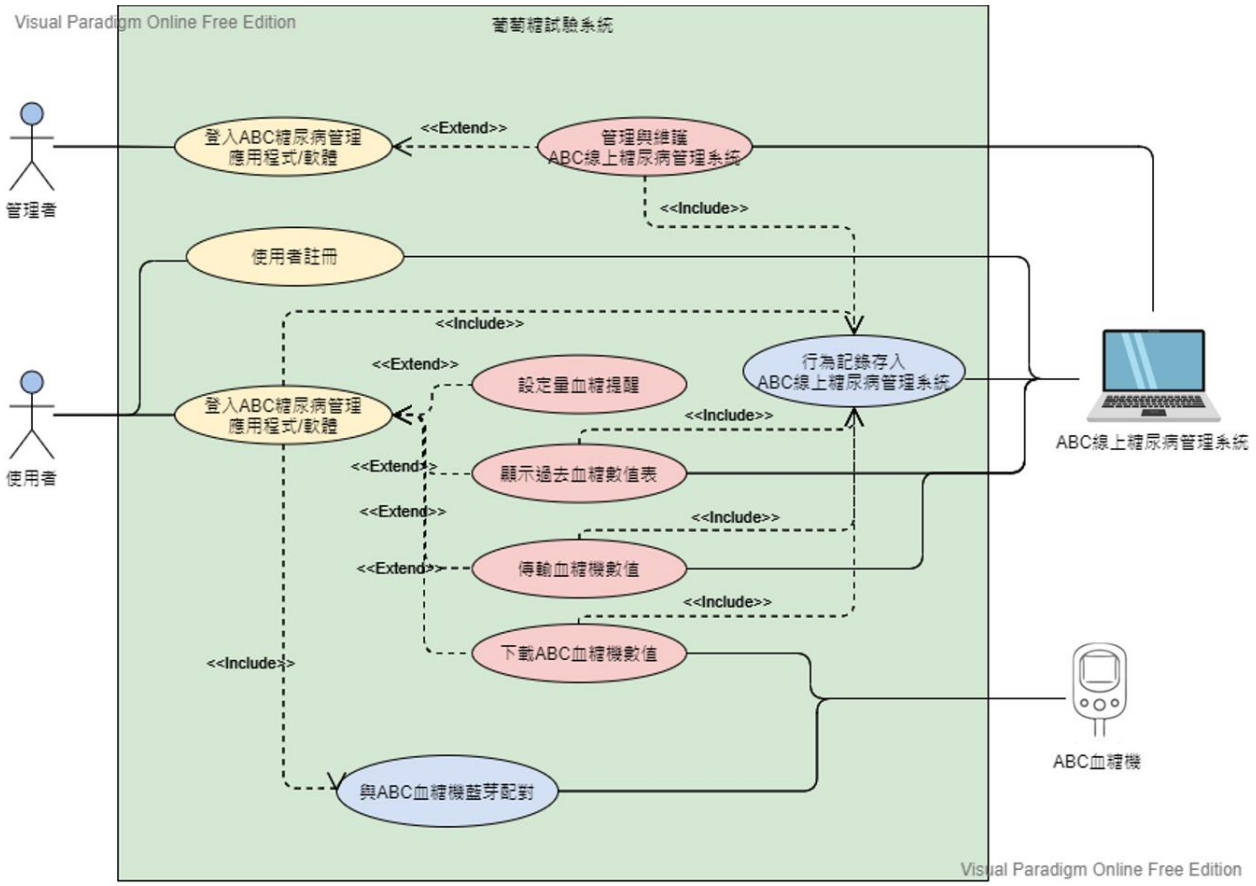


圖3.2.1、ABC葡萄糖試驗系統使用案例圖

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：

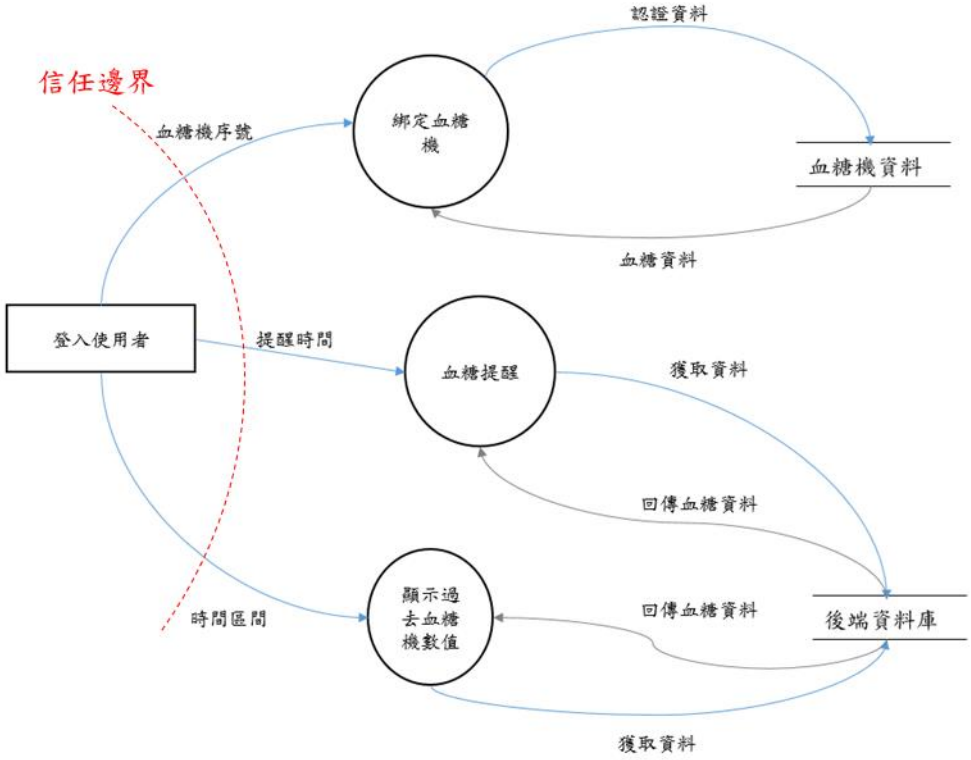


圖3.2.2、ABC葡萄糖試驗系統資料流向圖

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

本系統之威脅模型(Threat Model Diagram)，如下圖4所示:

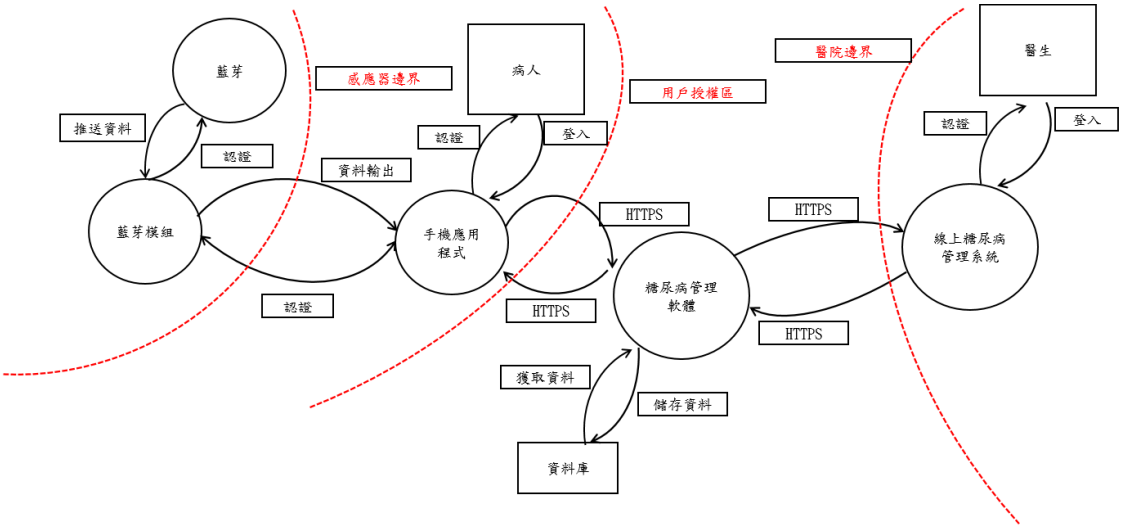


圖3.3.1、ABC葡萄糖試驗系統威脅模型

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葡萄糖試驗系統。
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。

缺陷通常可由安全修補程序、新的程式碼或硬體的變更來修補。

漏洞掃描測試報告如下圖3.5.1.1所示:

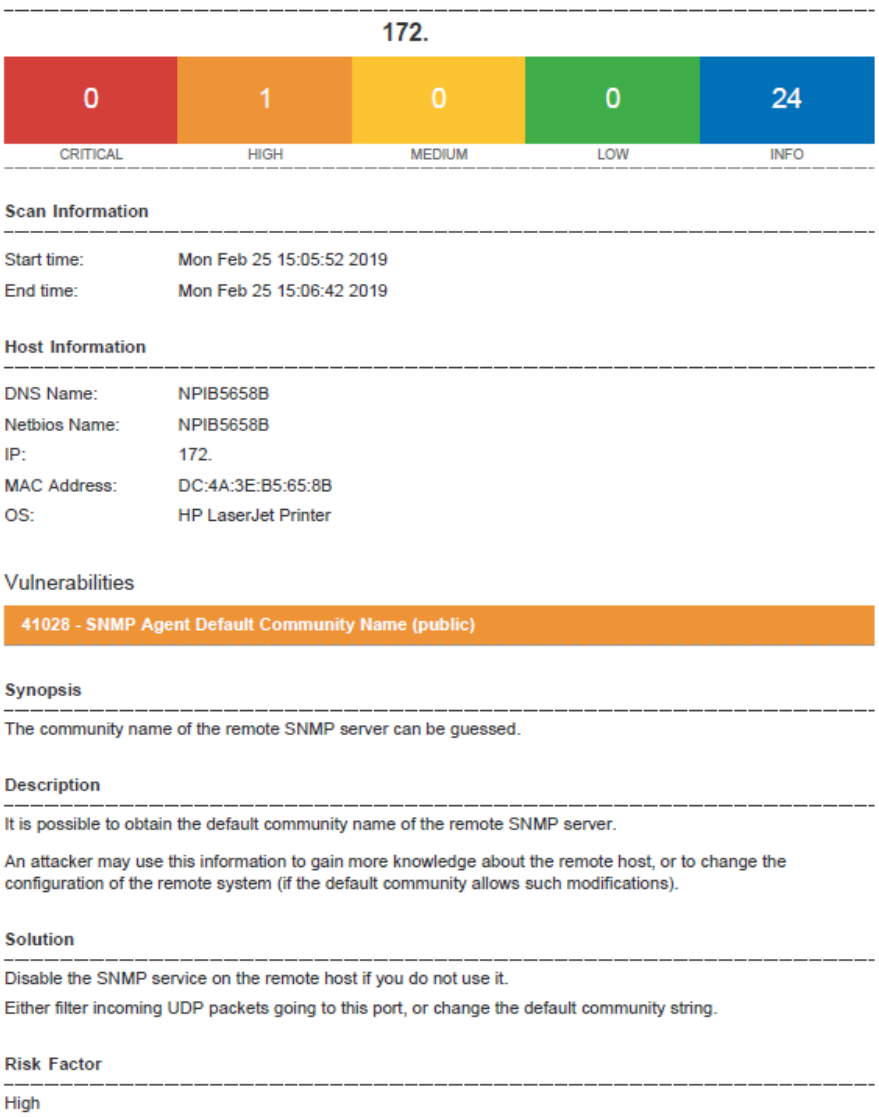


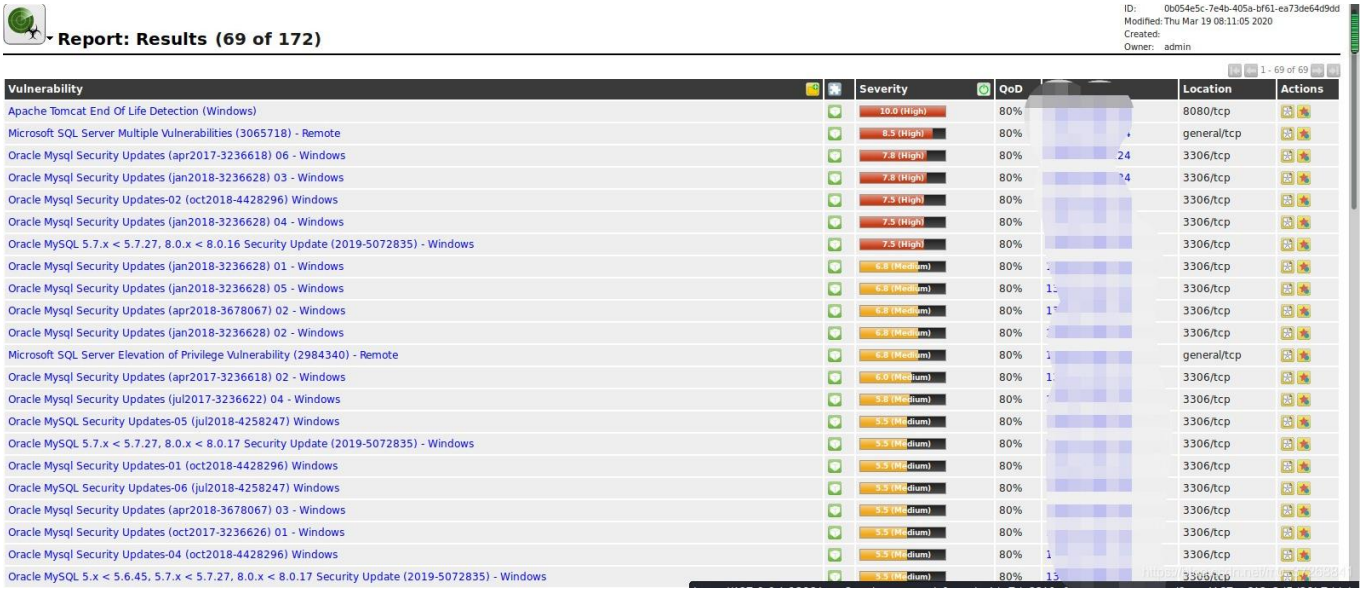
圖3.5.1.1、漏洞掃描測試報告圖

[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)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。

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)

美國 FDA 於 2019 年 6 月 27 日警告患者和醫療保健提供者關於 某些 Medtronic MiniMed™胰島素幫浦(如下附錄二圖1)有潛在的網路安全風險[8]。我國於 2019 年 07 月 31 日發出"美敦力迷你美" 體外胰島素幫浦(衛署醫器輸字第010235號)與“美敦力”迷你美波立得胰島素幫浦(衛署醫器輸字第022476號)等2張許可證安全警訊。上述 2 項產品被調查發現有潛在網路安全漏洞，未經授權且擁有特殊技術的人員，可能使用無線 網路技術連結後，改變幫浦設定和控制胰島素輸送。如果輸送過多的 胰島素可能導致低血糖；如果沒有輸送足夠的胰島素則可能導致高血 糖症和糖尿病酮症酸中毒。

附錄二圖1、Medtronic MiniMed™胰島素幫浦

目前市面上已有血糖機(例如 CONTOUR™ PLUS LINK 2.4)與美敦力 MiniMed 幫浦相連接(參考資料: https://www.fda.gov/medical- devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication)，血糖儀可以自動將血糖結果直接傳送到MiniMed 胰島素幫浦。不需要將血糖結果手動輸入胰島素幫浦。

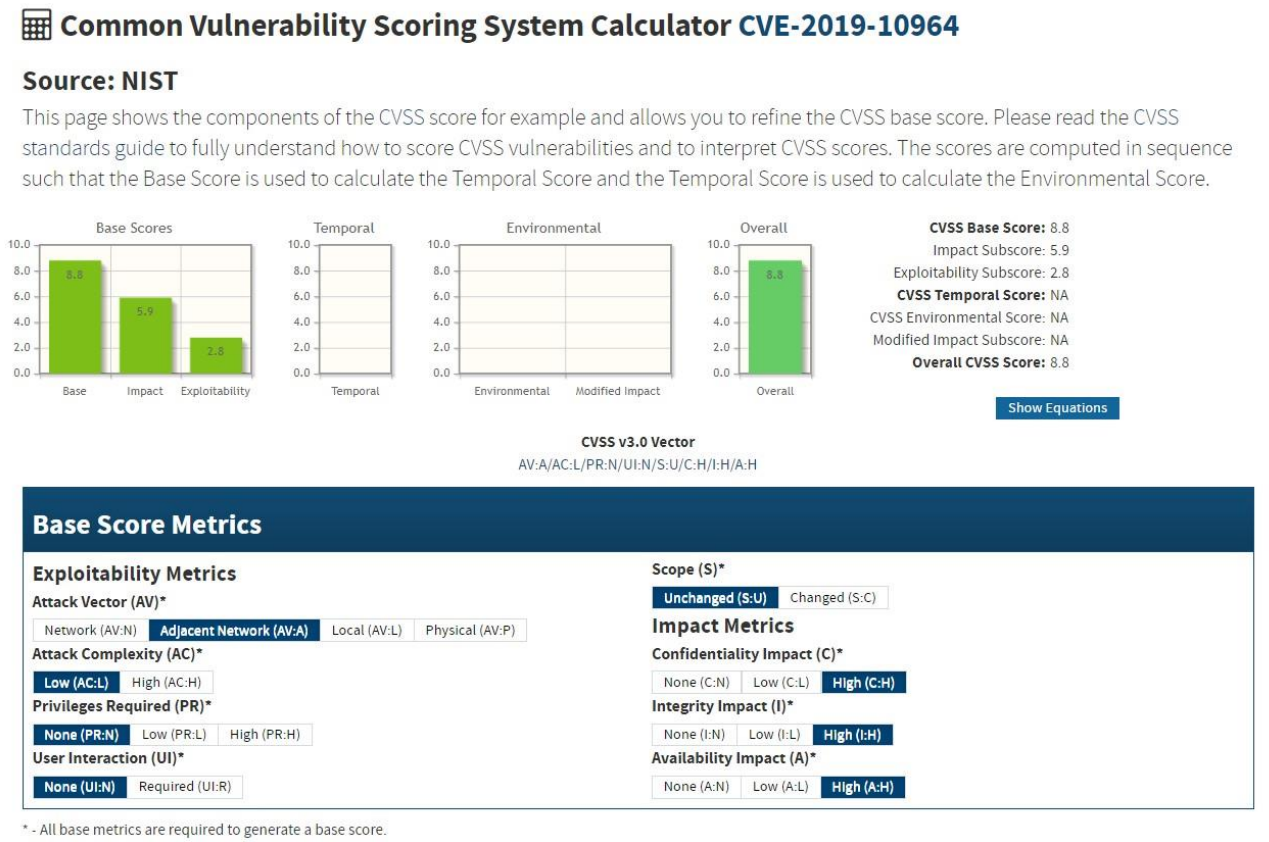
附錄二表1呈現美敦力之 MiniMed 於美國國家漏洞資料庫的資訊，附錄二圖2以CVE-2019-10964 為例呈現評估。

附錄二表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

[8] https://consumer.fda.gov.tw/Light/newsDetail.aspx?nodeID=217&id=4194

	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**



附錄二圖2、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(詳如附錄二表2)[9] [10]。

附錄二表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

[9] https://www.accessdata.fda.gov/cdrh_docs/pdf/P980016S436M.pdf
[10] 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)[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 Glucose (葡萄糖)關鍵字搜尋所獲得的資訊詳如附錄三表1，而Kotlin關鍵字搜尋所獲得的資訊詳如附錄三表2，OpenSSL關鍵字搜尋詳如附錄三表3，HTTP關鍵字搜尋則詳如附錄三表4。

附錄三表1、CVE 資料庫(關鍵字: Glucose)

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.
CVE-2017-5906	The Everyday Health Diabetes in Check: Blood Glucose & Carb Tracker app 3.4.2 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2017-13993	An Uncontrolled Search Path or Element issue was discovered in i-SENS SmartLog Diabetes Management Software, Version 2.4.0 and prior versions. An uncontrolled search path element

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

	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.

附錄三表2、Kotlin於美國國家漏洞資料庫的資訊(關鍵字: Kotlin)

漏洞編號	說明
CVE-2020- 15824	In JetBrains Kotlin from 1.4-M1 to 1.4- RC (as Kotlin 1.3.7x is not affected by the issue. Fixed version is 1.4.0) there is a script-cache privilege escalation vulnerability due to kotlin-main-kts cached scripts in the system temp directory, which is shared by all users by default. **Published:** August 08, 2020; 5:15:11 PM -0400
CVE-2020- 4072	In generator-jhipster-kotlin version 1.6.0 log entries are created for invalid password reset attempts. As the email is provided by a user and the api is public this can be used by an attacker to forge log entries. This is vulnerable to https://cwe.mitre.org/data/definitions/117. html This problem affects only application generated with jwt or session authentication. Applications using oauth are not vulnerable. This issue has been fixed in version 1.7.0. **Published:** June 25, 2020; 4:15:11 PM -0400
CVE-2019- 16303	A class generated by the Generator in JHipster before 6.3.0 and JHipster Kotlin through 1.1.0 produces code that uses an insecure source of randomness (apache.commons.lang3 RandomStringUtils). This allows an attacker (if able to obtain their own password reset URL) to compute the value for all other password resets for other accounts, thus allowing privilege escalation or account takeover. **Published:** September 13, 2019; 8:15:10 PM -0400
CVE-2019- 12845	The generated Kotlin DSL settings allowed usage of an unencrypted connection for resolving artifacts. The issue was fixed in JetBrains TeamCity 2018.2.3. **Published:** July 03, 2019; 4:15:11 PM -0400
CVE-2019- 10103	JetBrains IntelliJ IDEA projects created using the Kotlin (JS

	Client/JVM Server) IDE Template were resolving Gradle artifacts using an http connection, potentially allowing an MITM attack. This issue, which was fixed in Kotlin plugin version 1.3.30, is similar to CVE-2019- 10101. **Published:** July 03, 2019; 4:15:11 PM -0400
CVE-2019- 10102	JetBrains Ktor framework (created using the Kotlin IDE template) versions before 1.1.0 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack. This issue was fixed in Kotlin plugin version 1.3.30. **Published:** July 03, 2019; 4:15:11 PM -0400
CVE-2019- 10101	JetBrains Kotlin versions before 1.3.30 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack. **Published:** July 03, 2019; 4:15:11 PM -0400

附錄三表3、OpenSSL 於美國國家漏洞資料庫的資訊(關鍵字: OpenSSL，共 336 筆，此表摘錄 20 筆)

漏洞編號	說明
CVE-2020-5992	NVIDIA GeForce NOW application software on Windows, all versions prior to 2.0.25.119, contains a vulnerability in its open-source software dependency in which the OpenSSL library is vulnerable to binary planting attacks by a local user, which may lead to code execution or escalation of privileges. **Published:** November 11, 2020; 6:15:11 PM -0500
CVE-2020-25646	A flaw was found in Ansible Collection community.crypto. openssl_privatekey_info exposes private key in logs. This directly impacts confidentiality **Published:** October 29, 2020; 4:15:19 PM -0400
CVE-2020-10139	Acronis True Image 2021 includes an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis True Image contains a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. **Published:** October 21, 2020;

	10:15:15 AM -0400
CVE-2020-10138	Acronis Cyber Backup 12.5 and Cyber Protect 15 include an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis Cyber Backup and Cyber Protect contain a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. **Published:** October 21, 2020; 10:15:15 AM -0400
CVE-2020-25644	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **Published:** October 06, 2020; 10:15:12 AM -0400
CVE-2020-7069	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data. **Published:** October 02, 2020; 11:15:12 AM -0400
CVE-2020-1968	The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v). **Published:** September 09, 2020; 10:15:12 AM -0400
CVE-2020-8023	A acceptance of Extraneous Untrusted Data With Trusted Data vulnerability in the start script of openldap2 of SUSE Enterprise Storage 5, SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11- SP4, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-

	SECURITY, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2- LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12- SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8; openSUSE Leap 15.1, openSUSE Leap 15.2 allows local attackers to escalate privileges from user ldap to root. This issue affects: SUSE Enterprise Storage 5 openldap2 versions prior to 2.4.41- 18.71.2. SUSE Linux Enterprise Debuginfo 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Debuginfo 11-SP4 openldap2 versions prior to 2.4.26 0.74.13.1,. SUSE Linux Enterprise Point of Sale 11-SP3 openldap2 versions prior to 2.4.26-0.74.13.1,. SUSE Linux Enterprise Server 11- SECURITY openldap2-client-openssl1 versions prior to 2.4.26-0.74.13.1. SUSE Linux Enterprise Server 11-SP4- LTSS openldap2 versions prior to 2.4.26- 0.74.13.1,. SUSE Linux Enterprise Server 12-SP2-BCL openldap2 versions prior to 2.4.41- 18.71.2. SUSE Linux Enterprise Server 12-SP2-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-BCL openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP3-LTSS openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP4 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server 12-SP5 openldap2 versions prior to 2.4.41- 18.71.2. SUSE Linux Enterprise Server 15-LTSS openldap2 versions prior to 2.4.46-9.31.1. SUSE Linux Enterprise Server for SAP 12-SP2 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 12- SP3 openldap2 versions prior to 2.4.41-18.71.2. SUSE Linux Enterprise Server for SAP 15 openldap2 versions prior to 2.4.46-9.31.1. SUSE OpenStack Cloud 7 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud 8 openldap2 versions prior to 2.4.41-18.71.2. SUSE OpenStack Cloud Crowbar 8 openldap2 versions prior to 2.4.41- 18.71.2. openSUSE Leap 15.1 openldap2 versions prior to 2.4.46- lp151.10.12.1. openSUSE Leap 15.2 openldap2 versions prior to 2.4.46- lp152.14.3.1.

	Published: September 01, 2020; 8:15:10 AM -0400
CVE-2020-24714	The Scalyr Agent before 2.1.10 has Missing SSL Certificate Validation because, in some circumstances, the openssl binary is called without the - verify_hostname option. **Published:** August 27, 2020; 6:15:09 PM -0400
CVE-2020-8224	A code injection in Nextcloud Desktop Client 2.6.4 allowed to load arbitrary code when placing a malicious OpenSSL config into a fixed directory. **Published:** August 10, 2020; 10:15:13 AM -0400
CVE-2020-14396	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference. **Published:** June 17, 2020; 12:15:11 PM -0400
CVE-2020-13962	Qt 5.12.2 through 5.14.2, as used in unofficial builds of Mumble 1.3.0 and other products, mishandles OpenSSL's error queue, which can cause a denial of service to QSslSocket users. Because errors leak in unrelated TLS sessions, an unrelated session may be disconnected when any handshake fails. (Mumble 1.3.1 is not affected, regardless of the Qt version.) **Published:** June 08, 2020; 8:15:10 PM -0400
CVE-2020-13417	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **Published:** May 22, 2020; 5:15:12 PM -0400
CVE-2020-1967	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f). **Published:** April 21, 2020; 10:15:11

	AM -0400
CVE-2020-11876	** DISPUTED ** airhost.exe in Zoom Client for Meetings 4.6.11 uses the SHA-256 hash of 0123425234234fsdfsdr3242 for initialization of an OpenSSL EVP AES-256 CBC context. NOTE: the vendor states that this initialization only occurs within unreachable code. **Published:** April 17, 2020; 12:15:13 PM -0400
CVE-2020-7224	The Aviatrix OpenVPN client through 2.5.7 on Linux, macOS, and Windows is vulnerable when OpenSSL parameters are altered from the issued value set; the parameters could allow unauthorized third-party libraries to load. **Published:** April 16, 2020; 3:15:34 PM -0400
CVE-2019-17185	In FreeRADIUS 3.0.x before 3.0.20, the EAP-pwd module used a global OpenSSL BN_CTX instance to handle all handshakes. This mean multiple threads use the same BN_CTX instance concurrently, resulting in crashes when concurrent EAP-pwd handshakes are initiated. This can be abused by an adversary as a Denial-of- Service (DoS) attack. **Published:** March 20, 2020; 9:15:12 PM -0400
CVE-2019-14887	A flaw was found when an OpenSSL security provider is used with Wildfly, the 'enabled-protocols' value in the Wildfly configuration isn't honored. An attacker could target the traffic sent from Wildfly and downgrade the connection to a weaker version of TLS, potentially breaking the encryption. This could lead to a leak of the data being passed over the network. Wildfly version 7.2.0.GA, 7.2.3.GA and 7.2.5.CR2 are believed to be vulnerable. Published: March 16, 2020; 11:15:12 AM -0400
CVE-2020-9434	openssl_x509_check_ip_asc in lua- openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non- boolean return values. **Published:** February 27, 2020; 6:15:13 PM -0500
CVE-2020-9433	openssl_x509_check_email in lua- openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non- boolean return values. **Published:** February 27, 2020; 6:15:13 PM -0500

附錄三表4、HTTPd於美國國家漏洞資料庫的資訊(關鍵字: Apache httpd，共217筆，此表摘錄20筆)

漏洞編號	說明
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers. **Published:** August 07, 2020; 12:15:12 PM -0400
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers. **Published:** August 07, 2020; 12:15:11 PM -0400
CVE-2020-11985	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020. **Published:** August 07, 2020; 12:15:11 PM -0400
CVE-2020-11984	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE **Published:** August 07, 2020; 12:15:11 PM -0400
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL. **Published:** April 01, 2020; 8:15:13 PM -0400
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server. **Published:** April 01, 2020; 4:15:15 PM -0400
CVE-2020-1938	When using the Apache JServ Protocol (AJP), care must be

	taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.1.99 , Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence- in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.1.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations. **Published:** February 24, 2020; 5:15:12 PM -0500
CVE-2019-10097	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients. **Published:** September 26, 2019; 12:15:10 PM -0400
CVE-2019-10092	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. **Published:** September 26, 2019; 12:15:10 PM -0400

CVE-2019-10082	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown. **Published:** September 26, 2019; 12:15:10 PM -0400
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. **Published:** September 25, 2019; 1:15:10 PM -0400
CVE-2019-10081	HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client. **Published:** August 15, 2019; 6:15:12 PM -0400
CVE-2019-9517	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both. **Published:** August 13, 2019; 5:15:12 PM -0400
CVE-2019-13035	Artica Pandora FMS 7.0 NG before 735 suffers from local privilege escalation due to improper permissions on C:\PandoraFMS and its sub-folders, allowing standard users to create new files. Moreover, the Apache service httpd.exe will try to execute cmd.exe from C:\PandoraFMS (the current directory) as NT AUTHORITY\SYSTEM upon web requests to the portal. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. **Published:** June 29, 2019; 9:15:08 AM -0400
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server

	that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue. **Published:** June 11, 2019; 6:29:04 PM -0400
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly. **Published:** June 11, 2019; 6:29:03 PM -0400
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them. **Published:** June 11, 2019; 5:29:00 PM -0400
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **Published:** April 08, 2019; 6:29:00 PM -0400
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **Published:** April 08, 2019; 5:29:00 PM -0400
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions. **Published:** April 08, 2019; 4:29:10 PM -0400