財團法人醫藥品查驗中心 Center for Drug Evaluation, Taiwan 當代醫藥法規月刊 2021-11-10 133
回 CDE 官網首頁 訂閱/取消電子報

美國 FDA 於 2021 年 8 月發表「加強醫療器材服務相關網路安全規範」討論文章

發表單位：	美國 FDA	摘要整理：	顧國暐
發表時間：	2021/08/12	內容歸類：	醫療器材
類　　別：	討論文章	關 鍵 字：	Cybersecurity、Privileged Access

資料來源： Discussion Paper: Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities

重點內容：

1. 本篇文章主要在探討醫療器材由非原始設備製造商(non-OEMs)進行除錯、保養、維修等服務作業時，所衍生之網路安全議題。適用產品範圍包含由軟體驅動之醫療器材(包含韌體)或可程式化邏輯(programmable logic)、醫療器材軟體(SaMD)，及作為可相互操作系統(interoperable system)部件之器材。
2. 醫療器材網路安全之挑戰與展望
   (1) 特權存取(Privileged Access)：
   使用者存取權之限制，將扮演維護醫療器材網路安全之重要角色。原始設備製造商應設計使用者驗證(user authentication)等機制，確保僅特定實體(entity)具有產品操作系統之存取權，在盡可能不影響產品使用安全及效能前提下，提升產品資訊安全並減低未授權存取之發生。
   (2) 辨識網路安全弱點與資安事件：
   資安事件之偵測與應對向來是一項挑戰。提供醫療器材維護服務的實體因其於產業鏈中的定位，可以協助提早發現產品的網路安全弱點，有時甚至可早於原始設備製造商(OEM)。這些實體若可將取得的產品上市後資訊分享至 OEM、FDA、資訊共享與分析組織(ISAOs)及國土安全部(DHS)等利害關

係人(stakeholders)，將有助於提前偵測到網路安全弱點並研擬應對措施，進而降低資安風險。

(3) 預防與減緩網路安全弱點：

軟體更新或升級是應對病毒、惡意程式，或其他網路安全弱點之常見方式。提供醫療器材維護服務的實體因其於產業鏈中的定位，可協助確保產品軟體更新至最新版本，以維持產品的網路安全。及時導入經驗證的更新軟體對於減輕網路安全風險是十分關鍵的，因此建議 OEM 可與醫療器材服務實體合作，落實網路安全維護作業。

(4) 已終止生命週期產品面臨之挑戰與展望：

即使產品仍保有原廠規格之安全與效能，不再接受更新或補強之軟體將難以對抗日新月異的網路攻擊危害，因此當原始設備製造商無法或決定不再支援軟體更新服務，應通知客戶產品之生命週期與服務即將終止。基於醫療機構(health establishments)等用戶難以預測廠商告知終止服務的時間，用戶得以責任協議(responsibility agreements)方式保留性能符合規格要求之產品，但仍應留意產品所面臨的資安風險，並針對潛在風險研擬應對措施。

3. 指出醫療器材網路安全與維護服務相關之挑戰，有助於將利益最大化，並將病人承受之風險降至最低。因此 FDA 希望獲得利害關係人對於以下議題之意見：

(1) 現今與醫療器材維護服務相關之網路安全挑戰與展望為何？

(2) 前述四項論點是否為現今醫療器材維護服務涉及之主要網路安全議題？如果不是，則應著重於哪些論點？

(3) 提供醫療器材維護服務的實體能以哪些方式協助加強醫療器材網路安全？