# 廣泛使用的第三方軟體組件有 URGENT/11 網路安全弱點(Cybersecurity Vulnerabilities)而可能引發某些醫療器材使用期間的風險

## 安全警訊

（通類產品）

**警訊摘要：**

美國食品藥物管理局（FDA）提醒患者、醫療保健提供者、醫事機構人員和製造商注意網路安全弱點，可能會引發某些醫療器材與醫院網路的風險。FDA 尚未得知確定與這些網路弱點相關的不良事件，但是含有這些弱點的軟體已經公開可用。

安全研究人員已識別出名為 Urgent/11 的 11 個網路弱點，這些弱點可能使任何人以遠端控制醫療器材並更改其功能，導致服務拒絕，抑或導致資訊洩漏或邏輯缺失，進而可能妨礙器材功能。

這些弱點存在於支援電腦間網路通訊的 IPnet 第三方軟體組件。儘管初始的軟體供應商可能不再支援 IPnet 軟體，但是部分業者已取得執照，允許其在未有支援的情況下繼續使用該軟體。因此，該軟體可以被結合到可以在當今仍在使用的各種醫療和工業設備中使用的其他軟體應用、設備和系統中。

安全研究人員、醫療器材製造商及 FDA 已注意到以下操作系統的部分版本會受到影響。請注意，有弱點的 IPnet 軟體組件可能未包含於這些作業系統的所有版本中：

- VxWorks (by Wind River)
- Operating System Embedded (OSE) (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)

部分醫療器材製造商已在積極評估哪些使用這些作業系統的設備會受到 Urgent/11 的影響，並確定風險和補救措施。幾家製造商已將目前為止確定為受影響的設備通知客戶，其中包括影像系統、輸液幫浦和麻醉機。FDA 預計將鑑別出更多醫療器材，含有與初始 IPnet 軟體相關的一個或多個弱點。

**FDA 給製造商的建議：**

- 按照 FDA 網路安全後市場指引中的敘述進行風險評估，以評估這些弱點對醫療設備產品組合的影響並擬定風險降低計畫。請記住，這些弱點的性質使得攻擊不會被發現且無需使用者的互動。由於受影響的設備可能會將攻擊解釋為正常的和良性的網路通訊，因此對於現有的安全措施而言，攻擊可能仍然不可見。
- 與作業系統供應商合作，以確定是否有修補程式(patch)並實施建議的緩解方法。醫療器材製造商將需要評估和驗證設備的修補程式。
- 確保當前可能採用的任何緩解措施（例如：防火牆、虛擬私人網路(VPN)）不受 Urgent/11 的影響。
- 擬定計畫更新醫療設備，以相容不受 URGENT / 11 漏洞影響的 OS 版本（或通訊協定）。

**FDA 給醫療保健提供者的建議：**

- 對於使用可能受影響醫療器材的病人給予建議。
- 提醒使用醫療器材的病人，如果他們認為醫療器材的操作或功能發生非預期變化，請立即尋求醫療協助。
- 與醫療器材製造商合作，找出您的設施中或患者使用的醫療器材可能會受到這些弱點的影響，並擬定風險降低計畫。

**FDA 給醫事機構員工的建議（包括資訊科技人員）：**

- 監控您的網路流量與日誌(Log)，以察覺發生 URGENT/11 攻擊的跡象。
- 使用防火牆、虛擬私人網路(VPN)或其他科技將 URGENT/11 弱點降至最低。

**FDA 給患者與護理人員的建議：**

- 與您的醫療保健提供者聯繫，查明您的醫療器材是否可能受到影響。請注意，在本則警訊發布時醫療保健提供者可能還未取得此資訊，當更多資訊可取得時，醫療器材製造商應聯繫其客戶。
- 如果您認為醫療器材的操作或功能發生非預期變化，請立即尋求醫療協助。

**相關警訊來源（網址）：**

美國 FDA：
https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce