Se revelaron múltiples vulnerabilidades de seguridad en las bombas de infusión conectadas a Internet de Baxter, que utilizan los profesionales de la salud en entornos clínicos para dispensar medicamentos a los pacientes.

> *«La explotación exitosa de estas vulnerabilidades podría resultar en el acceso a datos confidenciales y la alteración de la configuración del sistema»,* dijo la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA).

Las bombas de infusión son dispositivos habilitados para Internet que usan los hospitales para la administración de medicamentos y nutrición directamente en el sistema circulatorio de un paciente.

Las cuatro vulnerabilidades en cuestión, descubiertas por la empresa de seguridad cibernética Rapid7 e informadas a Baxter en abril de 2022, afectan a los siguientes sistemas Sigma Spectrum Infusion:

- Sigma Spectrum v6.x modelo 35700BAX
- Sigma Spectrum v8.x modelo 35700BAX2
- Baxter Spectrum IQ (v9.x) modelo 35700BAX3
- Módulos de batería inalámbrica Sigma Spectrum LVP v6.x v16, v16D38, v17, v17D19, v20D29 a v20D32 y v22D24 a v22D28
- Módulos de batería inalámbrica Sigma Spectrum LVP v8.x v17, v17D19, v20D29 a v20D32 y v22D24 a v22D28
- Baxter Spectrum IQ LVP (v9.x) con módulos de batería inalámbrica v22D19 a v22D28

La lista de vulnerabilidades descubiertas es:

- CVE-2022-26390 (puntaje CVSS: 4.2): Almacenamiento de credenciales de red e información de salud del paciente (PHI) en formato no cifrado
- CVE-2022-26392 (puntaje CVSS: 2.1): Una vulnerabilidad de cadena de formato cuando se ejecuta una sesión de Telnet

- CVE-2022-26393 (puntaje CVSS: 5.0): Una vulnerabilidad de cadena de formato al procesar información de SSID de WiFi
- CVE-2022-26394 (puntaje CVSS: 5.5): Falta de autenticación mutua con el host del servidor de puerta de enlace

La explotación exitosa de las vulnerabilidades anteriores podría causar una denegación de servicio (DoS) remota, o permitir que un atacante con acceso físico al dispositivo extraiga información confidencial, o de forma alternativa, lleve a cabo ataques de adversario en el medio.

Las vulnerabilidades podrían dar como resultado una *«pérdida de datos críticos de contraseña de WiFi, lo que podría conducir a un mayor acceso a la red si la red no se segmenta adecuadamente»*, dijo Deral Heiland, investigador principal de seguridad para IoT en Rapid7.

Baxter, en un aviso, enfatizó que los problemas solo afectan a los clientes que usan las capacidades inalámbricas del sistema de infusión Spectrum, pero también advirtió que podría provocar un retraso o interrupción de la terapia si las fallas se utilizan maliciosamente.

> *«Si se explotan, las vulnerabilidades podrían provocar la interrupción de la operación, la desconexión del WBM de la red inalámbrica, la alteración de la configuración del WBM o la exposición de los datos almacenados en el WBM»,* dijo la compañía.

Los últimos hallazgos son otra indicación de cómo las vulnerabilidades de software comunes siguen afectando a la industria médica, un desarrollo preocupante dadas las posibles implicaciones que afectan la atención al paciente.

Baxter recomienda a los clientes que se aseguren de que todos los datos y configuraciones se borren de las bombas fuera de servicio, coloquen los sistemas de infusión detrás de un firewall, hagan cumplir la segmentación de la red y utilicen protocolos sólidos de seguridad

de la red inalámbrica para evitar el acceso no autorizado.

> *«Es fundamental implementar procesos y procedimientos para administrar la desactivación de la tecnología médica, y garantizar que la PII y/o los datos de configuración, como WiFi, WPA, PSK, etc., se eliminen de los dispositivos antes de reventa o transferencia a otra parte»,* dijo Heiland.

> *«Mantenga una fuerte seguridad física dentro y alrededor de las áreas médicas que contienen dispositivos MedTech, así como áreas con acceso a una red biomédica. Implemente la segmentación de red para todas las redes biomédicas para evitar que otras redes generales o comerciales se comuniquen con dispositivos MedTech».*