Product Security Bulletin

Title: Spectrum V6/V8/IQ WBM Vulnerabilities
Publication Date: September 8, 2022
Updated August 3, 2023

Background

This notification applies to customers that utilize Baxter Spectrum Infusion System's Wireless Battery Module (WBM). The notification provides product security information and recommendations for security vulnerabilities in the Spectrum WBM. The vulnerabilities are described in ICS Advisory ICSMA-22-251-01 (https://www.cisa.gov/uscert/ics/advisories/ICSMA-22-251-01)

Baxter's Spectrum Infusion System is comprised of the Spectrum Large Volume Pump (LVP) and the Spectrum WBM, an external add-on to the Spectrum LVP that is used for wireless communication. The vulnerabilities affect the WBM. Therefore, Baxter customers who use the Spectrum WBM with the Spectrum LVP to facilitate Wi-Fi connectivity could potentially be impacted by these vulnerabilities. These vulnerabilities do not directly affect any hardware or software component on the Spectrum pump itself.

Affected Products

This notification applies to customers that utilize all versions of the Spectrum WBM as listed below:

- 35083 – b wireless battery module
- 35162 – b/g wireless battery module
- 35195 – a/b/g/n wireless battery module
- 35223 – a/b/g/n wireless battery module
- 36010 – a/b/g/n wireless battery module

This vulnerability does not apply to customers who do not use the wireless capabilities of the Baxter Spectrum Infusion System.

Versions of the Baxter Spectrum Infusion System that could utilize the affected WBM include Sigma Spectrum (v6.x), Sigma Spectrum (v8.x), and Baxter Spectrum IQ (v9.x).

Vulnerability Details

The Spectrum Wireless Battery Module (WBM) is affected by the following 4 vulnerabilities that, if exploited, could potentially allow access to sensitive data on the WBM and a failed network connection to the host gateway: CVE-2022-26390, CVE-2022-26392, CVE-2022-26393, CVE-2022-26394.

The worst case CVSS score of 5.5 has a vector of (AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).

Rationale for worst case CVSS score: Exploitation of this vulnerability would require accessibility to the same network that the device is connected to, for example the local Wi-Fi, or for devices to be configured for host-name resolution of the Baxter Gateway using an external DNS server outside of a customer's firewall. This scoring rating considers the attack complexity to be low, based on the conclusion that specialized access conditions and/or extenuating circumstances are not needed. The CVSS scoring also considered that no user privileges or interaction are required to exploit this vulnerability, and that sensitive data (e.g., network credentials) stored in RAM on the impacted device could be exposed.

The remaining vulnerabilities have lower CVSS scores.

Potential Impact on Performance, Safety and Data

If exploited, the vulnerabilities could result in disruption of WBM operation, disconnection of the WBM from the wireless network, alteration of the WBM's configuration, or exposure of data stored on the WBM. For customers using Spectrum IQ (v9.x) with Auto Programming, disruption of the wireless connectivity of the device could interrupt the Auto Programming capabilities of the system.

In a worst-case situation where the Spectrum WBM vulnerabilities are successfully exploited, a delay or interruption of therapy could result from disruption of the WBM functionality. Specifically, exploited vulnerabilities could result in:

- Prevention of the delivery of a Drug Library to the Spectrum LVP from the WBM or delivery of a modified Drug Library.
- For those Spectrum IQ (v9.x) systems configured for Auto Programming, disconnection of the WBM from the wireless network, preventing Auto Programming orders from being delivered.
- For those Spectrum IQ (v9.x) systems configured for Auto Programming, disclosure of the Patient ID stored in RAM on the WBM.

Baxter considers the risk of these vulnerabilities to be 'controlled' per guidance in FDA Postmarket Management of Cybersecurity in Medical Devices.

Response

Baxter Sigma Spectrum v8.x and Spectrum IQ (v9.x) Operator Manuals recommend customers implement countermeasures to increase the security of Spectrum Infusion System, such as placing the WBM behind the hospital's network firewall and isolating it on its own secure VLAN to segregate the system from other hospital systems.

Software updates to disable Telnet and FTP (CVE-2022-26392) were issued in WBM version 22D29. Software updates to address the format string attack (CVE-2022-26393) are included in WBM version 20D30 and all other WBM versions. Authentication is already available in Spectrum IQ (CVE-2022-26394). Instructions to erase all data and settings for WBMs and pumps before decommissioning and transferring to other facilities (CVE-2022-26390) are in process for incorporation into the Spectrum Operator's Manual and provided in the Migrations section below.

Mitigations & Compensating Controls

The following mitigations, in conjunction with the customer's own network security policies, reduce the likelihood that these vulnerabilities will be exploited:

- Baxter recommends that when Spectrum Pumps and WBMs are decommissioned, all data and settings should be erased, similar to how data on laptops and smartphones need to be erased before selling or giving away.

  To erase all data and settings on the pump to be decommissioned:
  1. Reset the network settings (Biomed->Network Configuration->Transfer Network Settings->Reset).
  2. Delete the drug library
  3. Clear the history log

  To erase all data and settings on the WBM to be decommissioned:
  1. Select a pump other than the one last used with the WBM.
  2. Reset the network settings AND enable networking on the pump.
  3. Place the WBM on the pump.
  4. Wait until the network icon turns yellow.

- Baxter strongly recommends placing Spectrum Infusion Systems behind the hospital's network firewall. Spectrum IQ and Spectrum v8 labeling recommends placing the Spectrum Infusion System on a secured separate VLAN with controlled access.

- Baxter recommends isolating the Spectrum Infusion Systems to its own network VLAN to segregate the system from other hospital systems and reduce the probability that a threat actor could execute an adjacent attack such as a Man in the Middle (MiTM) attack against the system.

- Baxter recommends using strongest available wireless network security protocols (WPA2, EAP-TLS, etc.) to prevent unauthorized access to your wireless network.

- If customers are using host-name resolution for the WBM to access the Baxter Gateway, customers should only use an internal DNS only for name resolution.

- As a last resort, customers may disable wireless operation of the Spectrum LVP. The Spectrum Infusion System was designed to operate without network access. This action would impact an organization's ability to rapidly deploy drug library (formulary) updates to their Spectrum LVPs.

For More Information

If you observe any symptoms that are representative of these vulnerabilities, disable wireless operation of your pump and contact your service representative immediately.

Additional resources:

https://www.cisa.gov/uscert/ics/advisories/ICSMA-22-251-01

For more information:

For Baxter technical support contact: 1-800-356-3454 (Prompt 1) or via email at: spectrumsupport@baxter.com

For questions regarding cybersecurity of Spectrum pumps or any Baxter product contact: productsecurity@baxter.com