Product Security Bulletin

Title: Spectrum V6 and V8 Advisory ICSMA-20-170-04
Publication Date: June 18, 2020

Updated: June 18, 2020

In support of our mission of saving and sustaining lives, Baxter takes product security seriously. Baxter has reviewed the Spectrum product line for cybersecurity related vulnerabilities and is voluntarily disclosing the following vulnerabilities per our responsible disclosure process.

Vulnerability Summary

The following vulnerabilities were identified in the Spectrum Infusion System(s) v6.x and v8.x. There have been no reports of the following vulnerabilities being exploited. Baxter has previously disclosed vulnerabilities in Sigma Spectrum v6.05.11 with 802.11 b/g Wireless Battery Module v16 in ICSA-15-181-01.

CVE-2020-12039 – A threat actor with physical access to a version 6.x or version 8.x Spectrum LVP and knowledge of the hard-coded PIN could log into the Biomed Options menu(s) on the device keypad using the hard-coded PIN and access features in those menus.

The Biomed Options menus allow users to change certain device settings, calibration settings, and network configuration of the device. Access to these menus does not expose any sensitive data (passwords) or PHI.

Affected Configuration(s):

- Sigma Spectrum Large Volume Pump (LVP) v6.x
- Baxter Spectrum Large Volume Pump (LVP) v8.x

CVE-2020-12040 – The Spectrum LVP with Wireless Battery Module (WBM) uses an un-encrypted (clear-text) and unauthenticated communication protocol at the application layer to communicate with the Baxter Gateway system. The un-encrypted and unauthenticated data is used to send infusion delivery status information and operational data. The data does not contain sensitive data (passwords) or PHI.

A threat actor with access to the network supporting the Spectrum system could view sensitive non-private data or execute a Man in the Middle (MiTM) attack to observe data sent between the Spectrum WBM and the Baxter Gateway.

Affected Configuration(s):

- Sigma Spectrum Large Volume Pump (LVP) v6.x
- Baxter Spectrum Large Volume Pump (LVP) v8.x

CVE-2020-12045 and CVE-2020-12041 – The Spectrum Wireless Battery Module operates a Telnet service on port 1023 with hard-coded credentials.

A threat actor with access to the network could access the command-line interface on the Wireless Battery Module, allowing them to access sensitive data (not including Wi-Fi PSK), temporarily modify the network configuration of the WBM, and reboot the WBM. The WBM does not contain PHI.

Note: this does not affect the Spectrum LVP the WBM is affixed to. This vulnerability only affects the WBM and rebooting the WBM does not impact operation of the LVP or interrupt therapy.

Affected Configurations:

- Baxter Spectrum Large Volume Pump (LVP) v8.x with Wireless Battery Modules (WBM) v17, v20D29, v20D30, v20D31, and v22D24

CVE-2020-12047 and CVE-2020-12043 – In the factory-default configuration, the Spectrum Wireless Battery Module operates an FTP service with hard-coded credentials.

When the Spectrum Wireless Battery Module is in its factory-default configuration, and then is subsequently configured for a non-factory-default wireless network, the FTP service operating in the Wireless Battery Module will remain operational until the WBM is rebooted.

Affected Configurations:

- Baxter Spectrum Large Volume Pump (LVP) v8.x with Wireless Battery Modules (WBM) v17, v20D29, v20D30, v20D31, and v22D24

Affected Products and Versions

The following product configurations are affected:

- Sigma Spectrum v6.x with Wireless Battery Modules v9, v11, v13, v14, v15, v16, v20D29, v20D30, v20D31, v22D24
- Baxter Spectrum v8.x with Wireless Battery Module v17, v20D29, v20D30, v20D31, and v22D24.

Mitigations

The following mitigations may be used by customers to reduce the likelihood that one of these vulnerabilities will be exploited:

- Baxter recommends ensuring appropriate physical controls within its customers environments to protect against unauthorized access to devices.

- 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 to observe clear-text communications.
- Baxter recommends using appropriate wireless network security protocols (WPA2, EAP-TLS, etc.) to provide authentication / encryption of wireless data sent to / from the Spectrum Infusion System.
- Customers should ensure the Wireless Battery Module is rebooted after configuration for their network(s) by removing the WBM from the rear of the Spectrum device for 10-15 seconds, and then re-attaching the WBM.
- Customers should always monitor for and/or block unexpected traffic, such as FTP, at network boundaries into the Spectrum-specific VLAN.
- As a last resort, customers may disable wireless operation of the pump. 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 pumps.
- Baxter has launched the Spectrum IQ Infusion System which does not contain any of the vulnerabilities defined in this bulletin.

Related 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.us-cert.gov/ics/advisories/icsma-20-170-04

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