Product Security Bulletin

Title: Treck TCP/IP Stack Vulnerabilities
Publication Date: June 16, 2020

Updated: July 15, 2020

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 Treck (https://treck.com) TCP/IP stack contained in the Digi (https://www.digi.com) Net+OS Operating System used in all versions of the Spectrum (WBM). These vulnerabilities are referred to commonly as the "Ripple20" (https://www.jsof-tech.com/ripple20/) series of vulnerabilities. The "Ripple20" vulnerabilities are not exclusive to Baxter or medical devices, and are described in ICS Advisory ICSA-20-168-01 (https://www.us-cert.gov/ics/advisories/icsa-20-168-01).

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 "Ripple20" vulnerabilities affect the Net+OS Operating System used in 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 third-party 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 14 of 19 reported "Ripple20" vulnerabilities that, if exploited, could potentially allow remote-code execution on the WBM and unauthorized data access: CVE-2020-11896, CVE-2020-11898, CVE-2020-11900, CVE-2020-11901, CVE-2020-11903, CVE-2020-11904, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, and CVE-2020-11914.

The Spectrum WBM does not use IPv6 or ethernet connectivity and therefore is not affected by the following "Ripple20" vulnerabilities: CVE-2020-11897, CVE-2020-11899, CVE-2020-11902, CVE-2020-11905, CVE-2020-11906.

The worst case CVSS score of 10.0 has a vector of AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Rationale: Exploitation of these vulnerabilities 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. The 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.

Potential Impact on Performance, Safety and Data

If exploited, the "Ripple20" vulnerabilities could result in an unauthorized user delivering code embedded as the payload of a packet, that may be executed by the WBM. This 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.

The "Ripple20" vulnerabilities do not allow the user to directly access or execute remote code on the Spectrum LVP itself. An unauthorized user would not be able to gain access to, or be able to execute remote commands on the Sigma Spectrum LVP. An unauthorized user would not be able to start, change or stop an infusion remotely.

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.
- Denial of Service attack resulting in an audible and visual watch dog error may lead to interruption of therapy based on this error.

Baxter considers the risk of the "Ripple20" vulnerabilities to be 'controlled' per guidance in FDA Postmarket Management of Cybersecurity in Medical Devices. Baxter has received no reports of exploits related to Baxter products being impacted by these vulnerabilities.

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.

Baxter has received a patch from the software vendor (Digi). This software patch has been released into manufacturing and service for the latest hardware/software configuration of the WBM (A/B/G/N – p/n 35223).

Mitigations & Compensating Controls

The following mitigations reduce the likelihood that the "Ripple20" vulnerabilities will be exploited:

- 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 appropriate 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.us-cert.gov/ics/advisories/icsa-20-168-01

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