Baxter Product Security Bulletin

RE: Treck TCP/IP Stack Vulnerabilities

Publication Date: June 16, 2020
Update Date: June 16, 2020

SUMMARY

Baxter is currently monitoring the recently published ICS-CERT Advisory (ICSA-20-168-01)[1], regarding multiple vulnerabilities affecting the embedded TCP/IP software created by Treck Inc (https://treck.com). This TCP/IP stack has been implemented in a wide variety of industries and products, including the Digi (https://www.digi.com) Net+OS operating system used in Baxter Spectrum Infusion System's Wireless Battery Modules.

The vulnerabilities (CVE-2020-11896 through CVE-2020-11914) vary in range from local attack to remote exploits that can target the vulnerable embedded TCP/IP stack. The vulnerabilities have been classified in (ICSA-20-168-01) as critical through low on the CVSS v3 rating scale. For a more detailed description of these vulnerabilities, it is recommended that customer view the information provided by Digi[2].

Baxter has conducted an in-depth analysis and determined all vulnerabilities in Baxter's battery modules are controlled per guidance in FDA Postmarket Management of Cybersecurity in Medical Devices. **Please note that vulnerabilities found in Digi Net+OS and Treck TCP/IP stack are not Baxter-specific vulnerabilities.**

AFFECTED PRODUCTS

The following Baxter Spectrum Infusion System's Wireless Battery Modules are impacted by the Treck TCP/IP vulnerabilities in Digi Net+OS:

- 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

RESPONSE

To date, Baxter has not received any reports of these vulnerabilities impacting clinical use of Baxter Spectrum Infusion Systems. Baxter has received a patch from the software vendor (Digi) and is performing appropriate verification and validation activities. Additional information will be released as it becomes available.

MITIGATIONS

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

---

[1] ICS-CERT: https://www.us-cert.gov/ics/advisories/icsa-20-168-01
[2] Digi: https://www.digi.com/support/knowledge-base/digi-international-security-notice-treck-tcp-ip-st

- 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.
- 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.

CONTACT 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