UPDATE: September 1, 2020

B. Braun Statement on Cybersecurity Vulnerability with Ripple20 Communications Software

Summary:

B. Braun Medical is aware of the Cybersecurity and Infrastructure Security Agency (CISA) notification concerning the Cybersecurity Vulnerability ICS-VU-035787 ICSA-20-168-01 Ripple20 reported by Treck Inc., a third party software vendor. The vulnerabilities exist in the third party software used for network communication. The Treck software is used in the B. Braun Outlook® ES Safety Infusion Pump System.

According to the CISA report, the vulnerability could affect a variety of devices in the marketplace and expose them to cybersecurity threats. The vulnerability is present because some medical devices utilize the Treck TCP/IP software stack in the medical device to communicate data with communication networks.

Affected Products:

B. Braun’s analysis determined that the Outlook 400ES infusion pump is the only product in our portfolio that uses the vulnerable source code in its wireless network communications software system. The specific vulnerabilities identified and CVSS scores are listed below.

The identified vulnerabilities do not provide a vector to control the Outlook 400ES remotely, nor alter medication dosages, nor allow the pump to be used as a gateway for network attack.

B. Braun Medical has conducted an in-depth analysis and determined that all vulnerabilities in the Outlook 400ES are rated as “controlled risk” as defined in FDA’s guidance Postmarket Management of Cybersecurity in Medical Devices.

The vulnerable software is not used in the Space® Infusion pump family (Infusomat® Space® Infusion Pump, Perfusor® Space® Syringe Pump, SpaceStation, and Space Wireless Battery), DoseTrac® Server, DoseLink Interface Software, Space Online Suite Server, Apex® Compounder and Pinnacle® Compounder.

Response:

To date, B. Braun has not received any reports of these vulnerabilities impacting the clinical use of the Outlook 400ES. B. Braun has analyzed the patches received from Treck and determined that the Outlook 400ES may be impacted by the following vulnerabilities. Note: the CVSS scores are values provided by Treck and we continue to evaluate their impact to the Outlook 400ES.

CVE-2020-11903 - scored by Treck Inc. with a CVSS value 6.5 (Medium Severity)
CVE-2020-11906 - scored by Treck Inc. with a CVSS value 6.3 (Medium Severity)
CVE-2020-11912 - scored by Treck Inc. with a CVSS value 5.3 (Medium Severity)
CVE-2020-11914 - scored by Treck Inc. with a CVSS value 4.3 (Medium Severity)
B. Braun continues to work with CISA, DHS and Treck to complete the vulnerability analysis of the software used in the Outlook 400ES infusion pump. B. Braun ensures high security standards throughout the product life cycle by using globally accepted standard test and verification methods. We have established processes to monitor the latest vulnerabilities, threats, or risks and will proactively implement measures as required.

Mitigations:

The following mitigations can be continued or deployed to reduce the risk that one of the identified vulnerabilities can be exploited;

- Place the pumps on a dedicated VLAN
- B. Braun recommends continuing to use appropriate wireless network encryption protocols (WPA-2, EAP, etc.) on the pump to prevent unauthorized wireless network access
- Verify network intrusion protection software, verify firewall settings, and if possible use network segmentation to prevent unauthorized network intrusion

No additional actions by our customers are recommended at this time.

References:

Further information can be found at the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security. (https://www.us-cert.gov/ics)

Please refer to the FDA’s guidelines on Postmarket Management of Cybersecurity in Medical Devices: https://www.fda.gov/media/95862/download