B. Braun Medical Inc.
824 12th Avenue
Bethlehem, PA 18018-0027
Telephone 610-691-5400
Fax: 610-997-4049

UPDATE: October 8, 2021

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 market place 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 **is not** impacted by the following vulnerabilities.

CVE Number	Treck Inc. CVSS Score	B. Braun Medical Inc. CVSS Score for the Outlook® ES Infusion System
CVE-2020-11903	6.5 (Medium Severity)	0.0 (None) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N

CVE Number	Treck Inc. CVSS Score	B. Braun Medical Inc. CVSS Score for the Outlook® ES Infusion System
CVE-2020-11906	6.3 (Medium Severity)	0.0 (None) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N
CVE-2020-11912	5.3 (Medium Severity)	0.0 (None) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N
CVE-2020-11914	4.3 (Medium Severity)	0.0 (None) CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N

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:

While B. Braun has determined that our devices are not impacted by the reported vulnerabilities, the following mitigations can be continued or deployed to reduce the risk of cyberattack;

- 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 required at this time. However, B. Braun has released the following software versions which include additional device enhancements which further secure the Outlook® ES Infusion System from the vulnerabilities identified by Treck Inc.:

- 151738 Rev A
- 151738 MP (Management Processor Software)

Users wishing to apply the software updates to their existing devices may contact B. Braun Medical Inc. by calling Infusion System Customer Support at: 1-800-627-7867. Note that due to the low impact and age of the Outlook® ES devices, service fees may apply.

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