B. Braun Medical Inc. Statement regarding cybersecurity vulnerability Nucleus TCP/IP Stack

Vulnerability Summary

B. Braun is aware of the cybersecurity issues identified by the firm Forescout Research Labs regarding 13 vulnerabilities in the Nucleus TCP/IP stack.

The vulnerabilities affect versions of the Nucleus Real-time Operating System (RTOS). Researchers have discovered vulnerabilities in multiple TCP/IP stacks in which ISNs (Initial Sequence Numbers within TCP connections) are improperly generated. This is leaving devices' TCP connections open to attacks.

B. Braun proactively analyzed the software stack of product lines that could potentially be affected by this vulnerability. **None** of the B. Braun products listed uses the operating systems detailed in the Forescout Research Labs communication.

Product lines include:

- Outlook® Safety Infusion System Pump family
- Space® Infusion Pump family (Infusomat® Space® Infusion Pump, Perfusor® Space® Infusion Pump, SpaceStation, and Space® Wireless Battery)
- DoseTrac® Server, DoseLink™ Server, and Space® Online Suite Server software
- Pinnacle® Compounder
- APEX® Compounder

B. Braun ensures high security standards throughout the product life cycle by using global accepted standard test and verification methods. It has established processes to monitor the latest vulnerabilities, threats, or risks and will proactively implement measures as required.

Further information can be found at the Department of Homeland Security Cybersecurity & Infrastructure Agency (CISA):

https://us-cert.cisa.gov/ncas/current-activity/2021/11/09/cisa-releases-security-advisory-siemens-nucleus-real-time