B. Braun Medical Inc. Statement regarding cybersecurity vulnerability in the InterNiche Technologies TCP/IP Stack

Vulnerability Summary

B. Braun is aware of the cybersecurity issues identified by the firm Forescout Research Labs regarding 14 vulnerabilities in the InterNiche Technologies TCP/IP stack.

INFRA:HALT is a set of 14 vulnerabilities jointly discovered by Forescout Research Labs and JFrog Security Research. It is part of Forescout's Project Memoria Research (Amnesia:33, NUMBER:JACK, NAME:WRECK) that focuses on the security of TCP/IP stacks. For further details please see https://www.forescout.com/research-labs/infra-halt/

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 TCP/IP software 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/ics/advisories/icsa-21-217-01v