B. Braun Medical Inc. Statement regarding cybersecurity vulnerabilities with Amnesia:33

Vulnerability Summary

B. Braun is aware of that the cybersecurity firm, Forescout Research Labs, has discovered a new set of 33 major vulnerabilities in Internet of Things (IoT), operational technology (OT) and IT devices impacting four widely used open-source TCP/IP stacks. These vulnerabilities reside in the uIP, FNET, picoTCP and Nut/Net stacks, which serve as foundational connectivity components for millions of IoT, OT, networking and IT devices. Four of these vulnerabilities are critical and allow for remote code execution.

B. Braun proactively analyzed the potential vulnerabilities and none of the B. Braun products listed below are impacted as they do not use any of the potentially impacted open-source TCP/IP stacks.

Product lines include:

- Outlook® Safety Infusion System Pump Family
- Space® Infusion Pump System (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

References:

Website Forescout Labs – Security Researcher AMNESIA:33 - Forescout