B. Braun Medical Inc. Statement regarding cybersecurity vulnerabilities concerning Name: Wreck

Vulnerability Summary

B. Braun is aware of that the cybersecurity firm, Forescout Research Labs, has discovered a new set of 9 vulnerabilities affecting Domain Name Systems (DNS) implementations.

These vulnerabilities relate to DNS implementations and can cause Denial of Service or Remote Code Execution, allowing attackers to take targeted IT, IoT or OT devices offline or take control of them. It affects four common TCP/IP stacks.

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 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 Name: WRECK - Forescout