

B. Braun Medical Inc. Statement regarding cybersecurity vulnerabilities identified by Palo Alto Networks

Vulnerability Summary

B. Braun is aware of the cybersecurity issues identified by the firm Palo Alto Networks described in a recent press release outlining the top 10 Infusion Pump vulnerabilities. The CVE (Common Vulnerabilities and Exposures) ID numbers are listed in the chart within the body of the press release.

B. Braun proactively analyzed the first two CVE numbers listed, CVE-2019-12255 and CVE-12264, at the time of notification. These pertained to 11 potential vulnerabilities within VxWorks software also known as 'Urgent 11'. The balance of the CVE numbers listed were reported by Becton Dickinson (3 through 5) and Baxter (6 through 10) regarding potential vulnerabilities within the software in their pump products.

None of the B. Braun products listed below are impacted by any potential vulnerability described in any of the CVEs outlined in the Palo Alto Networks press release.

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>

Additional information:

<https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/>

B. Braun Statement regarding 'Urgent 11' vulnerabilities

<https://www.bbraunusa.com/en/products-and-therapies/customer-communications.html>

Reference article: [B. Braun Medical Inc. Statement regarding cybersecurity vulnerability ICSMA-19-274-01 URGENT/11_11/04/2019](#)