COMPANY STATEMENT

October 1, 2019

Ensuring the safety and quality of our products is the top priority at BD, which is why we have a voluntary, proactive and coordinated vulnerability disclosure process to ensure our customers are aware of any potential vulnerabilities and the compensating controls to mitigate them, even when vulnerabilities exist in third-party software. As part of this commitment, BD has issued a product security bulletin for a previously disclosed third-party vulnerability that affects the Interpeak IPnet standalone TCP/IP networking software.

The facts of this vulnerability include:

- There have been no reported security incidents associated with this vulnerability in any BD products.
- The probability of harm is unlikely considering each individual device would need to be targeted via an exploit; there is a highly detectable audible and visual alarm and an exploit would not interrupt infusions.
- The compensating control for health care providers includes a simple firewall rule and can be found at www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/security-advisory-ipnet/.
- The medical benefits for continued use of the device outweigh the risks associated with these vulnerabilities.
- Additional mitigations can be found in BD's disclosure at https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletins/interpeak-ipnet-tcp-ip-stack-vulnerability.

BD is committed to being a transparent medical technology company regarding vulnerability disclosures, and we believe users of our technologies need to have clear and complete information regarding any potential vulnerability (including third-party software) to make rational decisions about the safe use of technology for patient care. BD will continue to take a leadership position in vulnerability disclosures.

# # #