CERT: AMENSIA:33 VULNERABILITIES IN MULTIPLE TCP/IP STACK SOFTWARE

Boston Scientific is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the December 9, 2020 announcement regarding the vulnerabilities of several open source Transmission Control Protocol/Internet Protocol (TCP/IP) embedded stacks

The following TCP/IP stacks are affected:

- uIP-Contiki-OS (end-of-life [EOL]), Version 3.0 and prior
- uIP-Contiki-NG, Version 4.5 and prior
- uIP (EOL), Version 1.0 and prior
- open-iscsi, Version 2.1.12 and prior
- picoTCP-NG, Version 1.7.0 and prior
- picoTCP (EOL), Version 1.7.0 and prior
- FNET, Version 4.6.3
- Nut/Net, Version 5.1 and prior

We have completed an analysis of our devices, digital health apps and remote monitoring services and have determined that our products are not impacted by these vulnerabilities.

For more detail, refer to:

- CISA: https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

Boston Scientific Corporation is committed to open communications with our customers and patients regarding product security. Please visit our Product Security website for additional security information, including how to contact us.

Revision 1 - March 15, 2021