

NAME: WRECK DNS 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 April 12, 2021 announcement regarding the vulnerabilities of several open source Transmission Control Protocol/Internet Protocol (TCP/IP) embedded stacks containing Domain Name Server (DNS) vulnerabilities.

The following types of TCP/IP stacks are affected by the vulnerabilities:

- FreeBSD (vulnerable version: 12.1)
- IPnet (vulnerable version: VxWorks 6.6)
- NetX (vulnerable version: 6.0.1)
- Nucleus NET (vulnerable version: 4.3)

Our global product cybersecurity team is in the process of assessing Boston Scientific products to determine if any are affected. As we complete this analysis, we will provide an update to this bulletin.

For more detail, refer to:

Health Sector Cybersecurity Coordination Center: <https://www.hhs.gov/sites/default/files/tlpwhite-hc3-analyst-note-name-wreck.pdf>

Please visit our [Product Security website](#) for additional security information, including how to contact us directly.

Revision 1 – April 29, 2021