CVE-2020-11898-11914 (AKA RIPPLE20)
NO INCREASED SECURITY RISK FROM TRECK, INC., EMBEDDED TCP/IP STACK VULNERABILITIES

The Boston Scientific team is dedicated to ensuring the safety and security of our products worldwide. Treck, Inc. informed us of vulnerabilities found in their software products which were identified by independent security research company JSOF. Boston Scientific uses portions of Treck TCP/IP software in all of our transvenous implantable cardiac devices as well as the associated device programmers located in physician offices and the LATITUDE™ Remote Patient Management Systems. We do not use Treck software in any subcutaneous implantable defibrillator systems (S-ICDs) or any other Boston Scientific products.

Boston Scientific has completed a risk assessment of the vulnerabilities that impact the Treck software used in our devices. We have concluded there is no increased security risk for patients who have our implantable products because of the Treck vulnerabilities. Our devices that utilize the impacted Treck software include additional security and privacy measures that prevent the disclosed vulnerabilities from affecting the performance of our products. Patients and physicians should continue normal use of the in-clinic programmers and at-home monitoring equipment.

Additional information about the safety of our affected products:
- The Treck software is only used for short distance communications between the implantable device, its associated in-clinic programmer and the LATITUDE remote patient management system.
- There is no ability to access the private communication channel between a device and the programmer or remote patient management system from the internet.
- Additional safeguards in the implantable devices prevent unauthorized changes to device settings to ensure devices will continue to function properly and without interruption.

We continue to work with Treck engineers to stay informed of the reported vulnerabilities and ensure the continued security and privacy of our products.

For more detail, refer to:
- Treck: https://treck.com/vulnerability-response-information/
- JSOF: https://www.jsof-tech.com/ripple20/

Revision 1 – June 25, 2020