ICS MEDICAL ADVISORY (ICSMA-19-274-01)
URGENT/11 - INTERPEAK IPNET TCP/IP STACK

The Boston Scientific team is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring cyber vulnerabilities called “URGENT/11” as identified by Armis, an enterprise Internet of Things (IoT) security company. Armis has also identified the source of the vulnerabilities - the IPnet TCP/IP stack created by a company called Interpeak.

Our product security team has conducted an analysis of our medical devices utilizing third-party operating systems and has confirmed that none of our devices use any version of the operating systems identified in these advisories. In addition, we have reviewed the software incorporated into our implantable medical devices and have confirmed our devices do not use the Interpeak IPnet TCP/IP stack.

We have identified two third-party firewall appliances manufactured by SonicWall that are impacted by the URGENT/11 vulnerabilities. These appliances are sold by Boston Scientific as optional Network Security Devices (NSDs) for customers who purchase our iLAB™ Ultrasound Imaging System and POLARIS™ Imaging System products. To date, we have not received any reports of this vulnerability being exploited in any of the deployed SonicWall NSD accessories we have sold and distributed.

We are working to provide updated and secure firewall capability to our Boston Scientific iLAB™ Ultrasound Imaging System and POLARIS™ Imaging System products, including:

- Deploying the SonicWall recommended software patches
- Replacing SonicWall NSDs that have been sold to our customers
- Updating our system software for additional security controls

We will be contacting customers with affected systems to schedule the update or replacement. If you would prefer to temporarily remove the impacted NSD until patching is performed, please contact Capital Equipment Technical Services for assistance.

Country/Continent	Telephone Number	Email	Fax Number
APAC	-64188813	CETechSupportAPAC@bsci.com	-15252
Australia/New Zealand	+61 1800 676 133 (option 5)	CapitalEquipmentANZ@bsci.com	1800 836 666
Austria	+43 1608 1037	CEtechsupportEMEA@bsci.com	+31 45 546 7805
Denmark	+45 80253429	CEtechsupportEMEA@bsci.com	+31 45 546 7805
Europe	+31 45 5467707	CETechSupportEMEA@bsci.com	+31 45 546 7805
Finland	+358 800770055	CEtechsupportEMEA@bsci.com	+31 45 546 7805
France	+33 139 304 971	CETechSupportEMEA@bsci.com	+31 45 546 7805
Germany	+49 815 126 86118	CETechSupportEMEA@bsci.com	+31 45 546 7805
Italy	+39 022 698 3218	CETechSupportEMEA@bsci.com	+31 45 546 7805
Japan	+81 44 287 7660	JapanCESTAC@bsci.com	-7916
Netherlands	+31 45 5467707	CEtechsupportEMEA@bsci.com	+31 45 546 7805
Norway	+47 80014236	CEtechsupportEMEA@bsci.com	+31 45 546 7805
Spain	+34 917 619 999	CETechSupportEMEA@bsci.com	+31 45 546 7805
United Kingdom	+44 1442 411 686	CETechSupportEMEA@bsci.com	+31 45 546 7805
U.S.	1-800-949-6708	CETechSupportUSA@bsci.com	510-952-3142
Argentina	+54-11-5777-2694	CustomerServiceArgentica@bsci.com	+54-11-57772680

Brazil	(+55)1155459064	CEBrazilTeam@bsci.com	-
Colombia	(+57)1-6295045	CustomerServiceColombia@bsci.com	-
Mexico	(+52)15559924100	CESupportMXC@bsci.com	-

Customers may also consider implementing detection and prevention methods in their enterprise firewall and intrusion detection systems. Armis has provided information to implement these detection and prevention methods on their website here.

For more detail of the vulnerabilities, please refer to the following sites:
ICS Advisory (ICSA-19-211-01) - https://www.us-cert.gov/ics/advisories/icsa-19-211-01
ICS Advisory - https://www.us-cert.gov/ics/advisories/icsa-19-274-01
SonicWall Notification - https://www.sonicwall.com/support/product-notification/?sol_id=190717234810906
Armis Website: https://www.armis.com/urgent11/

Revision 1 – January 3, 2020